AN AGGREGATED INFORMATION TECHNOLOGY CHECKLIST FOR OPERATIONAL RISK MANAGEMENT

MEHMET ZEKİ ÖNAL

BOĞAZİÇİ UNIVERSITY

2007

AN AGGREGATED INFORMATION TECHNOLOGY CHECKLIST FOR OPERATIONAL RISK MANAGEMENT

Thesis submitted to the

Institute for Graduate Studies in the Social Sciences

in partial fulfillment of the requirements for the degree of

Master of Arts

in

Management Information Systems

by

Mehmet Zeki Önal

Boğaziçi University

2007

Thesis Abstract

Mehmet Zeki Önal, “An Aggregated Information Technology Checklist for Operational Risk Management”

This paper develops an aggregated information technology (IT) checklist in order to manage the operational risks in an organization, especially those caused by the information systems and technology infrastructure. The study addresses the issue of the IT Governance frameworks and standards (information control models) that respond to different levels of operational risks and need to be harmonized. The definition of risk, operational risk, and risk management are discussed, a requirement analysis regarding Basel II is conducted, a gap analysis between the information control models (ICMs) is performed, and the aggregated IT checklist for operational risk management (ORM) is proposed by mapping the control objectives in ICMs to the operational risk categories described in Basel II as loss event types. The validity and reliability of the study is based on the focus group assessment of the mappings. The managerial impacts of the checklist are discussed, considering the audit implications of the checklist.

Tez Özeti

Mehmet Zeki Önal, “Operasyonel Risk Yönetimi için Bütünleştirilmiş Bilgi Teknolojileri Kontrol Listesi”

Bu makale, bir organizasyonda özellikle bilgi sistemleri ve teknolojileri altyapısından kaynaklanan operasyonel riskleri yönetebilmek amacıyla bütünleştirilmiş bir bilgi teknolojileri (BT) kontrol listesi geliştirmektedir. Çalışma, BT Yönetişim çerçevesi ve standartlarının (bilgi kontrol modelleri) farklı seviyelerdeki operasyonel risklere cevap vermeleri ve birleştirilmeleri gerektiğini sorununu vurgulamaktadır. Risk, operasyonel risk ve risk yönetimi tanımları tartışılmış, Basel II bağlamında bir gereksinim analizi yapılmış, bilgi kontrol modelleri (BKM) arasında bir farklılık analizi gerçekleştirilmiş ve Basel II’de zarar olay tipleri olarak açıklanan operasyonel risk kategorilerinin BKM’lerdeki kontrol hedeflerine eşleştirilmesi ile operasyonel risk yönetimi (ORY) için bütünleştirilmiş BT kontrol listesi önerilmiştir. Çalışmanın geçerliliği ve güvenilirliği, eşleştirmeler üzerinde yapılmış olan grup değerlendirmesine dayandırılmıştır. Kontrol listesinin yönetimsel etkileri, kontrol listesinin denetime etkileri göz önünde bulundurularak tartışılmıştır.

ACKNOWLEDGEMENTS

I would like to express my gratitude to a number of peoples, who helped me along the way, and made the accomplishment of this thesis possible. First of all, I would like to thank Assist. Prof. Ceylan Onay and Dr. Tamer Şıkoğlu, my advisors at the Department of Management Information Systems (MIS), for their encouragement, support, and feedback, and especially for sharing my enthusiasm.

I would also like to express my appreciation of my colleagues at the Systems and Process Assurance Department in PricewaterhouseCoopers Turkey, Seda Demircioğlu, Tumin Gültekin, Serdar Güzel, and Doğan Tanrıseven, for their interesting and inspiring thoughts, suggestions, and eminent supervision, especially while focusing on the principles of the study.

I would like to thank the focus group participants from Boğaziçi University, PricewaterhouseCoopers Turkey, and Opet Petrolcülük A. Ş. for sharing their ideas.

Finally, I would like to thank my parents, my sister, and my extended family members; numerous friends from high school and university; and my colleagues, who endured this long process with me, always offering support, clemency, and love.

CONTENTS

TABLES

FIGURES

ABBREVIATIONS

Abbreviation	Definition
AMA	Advanced Measurement Approach
BBA	British Bankers' Association
BI	Basic Indicator
BIS	Bank for International Settlements
BRSA	Banking Regulation and Supervision Agency
BS7799	British Standard 7799
BSI	British Standards Institute
CMMI	Capability Maturity Model Integration
CobiT	Control Objectives for Information and related Technology
COSO	Committee of Sponsoring Organizations
CRD	Capital Requirements Directive
DTI	United Kingdom Government's Department of Trade and Industry
ERM	Enterprise Risk Management
EU	European Union
EuroSox	European Sarbanes-Oxley (please refer to SAD)
GRC	Corporate Governance, Risk Management, and Regulatory Compliance
ICM	Information Control Model
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISDA	International Swaps and Derivatives Association
ISO	International Organization for Standardization
ISO27001	International Organization for Standardization's Standard 27001
IT	Information Technology
ITGI	Information Technology Governance Institute
ITGP	Information Technology Guiding Principle
ITIL	Information Technology Infrastructure Library
itSMF	Information Technology Service Management Forum
KPI	Key Performance Indicator
KRI	Key Risks Indicator
MAAP	Mission Assurance Analysis Protocol
OGC	United Kingdom's Office of Governance Commerce
ORM	Operational Risk Management
ORMMM	Operational Risk Management Maturity Model
PCAOB	Public Company Accounting Oversight Board
PwC	PricewaterhouseCoopers
QIS2	Quantitative Impact Study 2
RAROC	Risk Adjusted Return of Capital
RCSA	Risk and Control Self Assessment
RMA	Risk Management Association
RMG	Risk Management Group
SA	Standard Approach
SAD	Statutory Audit Directive
SAS	Statement of Audit Standard
SEC	Security Exchange Commission
SEI	Software Engineering Institute
US	United States
USA	United States of America
USC	United States Congress
VaR	Value at Risk

PREFACE

This master's thesis is the result of the study I have conducted in the period between August 2006 and June 2007 in combination with my occupation at the Systems and Process Assurance Department in PricewaterhouseCoopers Turkey. Since I have graduated from the Department of Management Information Systems at Boğaziçi University in 2004, I have found it inspiring to combine my business life and academic career by attending the master's program at the Department of Management Information Systems. Moreover, my dynamic working conditions stimulated my curiosity because I have attended lots of audit or advisory projects where the results of my study can be used effectively.

In addition, it was very motivating to be at Boğaziçi University again, after my undergraduate studies, to spend time in front of the Bosphorus at the South Campus, at the Management and Economics Club, and in other places in the university, to see old friends and tutors, and to participate in the graduation ceremony and to get a degree of Master of Arts.

Although I encountered some obstacles while writing this thesis, I am very glad to have been able to complete it in time, so that the results of the study will add a value to further academic researches, to the work of auditors and the business of auditees, since Basel II framework and information control models (ICMs) such as Control Objectives for Information and related Technology (CobiT) are hot topics in the business world in Turkey, the European Union, and the rest of the world.

The latest developments show us that the topic of this master's thesis was selected appropriately to comply with the needs of operational risk management (ORM), since the Information Systems and Control Association (ISACA) has published an exposure draft entitled Information Technology Control Objectives for Basel II and requested the feedback for the draft report until 18 June 2007 while I was writing these lines. Therefore, it was worth sacrificing my weekends, rest times, and even vacations for my research.

CHAPTER ONE

INTRODUCTION

The business environment is becoming more technologically powered and complex at each heartbeat. New risks and threats are being faced, the needs must be managed, and new opportunities are waiting to be tapped.

Operational risk is one of the most significant risks that businesses face in today's complex global economy (Samad-Khan, 2005). For most of the world's leading institutions it has become more than apparent that implementing an effective operational risk management (ORM) program can help reduce losses, lower costs associated with fixing problems and increase customer and employee satisfaction, thereby improving financial performance and enhancing shareholder value.

Thus, all these changes require and produce new regulations for framing and controlling the environment, such as Basel II capital allocation framework, which requires many actions at different levels in an organization. Basel II may have forced banks to review their approach to managing operational risk since it has been effective from 1 January 2007 in European countries. In addition, the Banking Regulation and Supervision Agency (BRSA) in Turkey announced in May 2005 that Basel II regulations for the Turkish banking sector would be effective beginning from 1 January 2008 within an ongoing process.

Basel II defines principles and sets rules for companies. Since Basel II requires a supervisory review process including the assessment of the control environment, it is also required that supervisors should consider the quality of the bank's management

information reporting and systems, the manner in which business risks and activities are aggregated, and the management's record in responding to emerging or changing risks (Basel Committee, 2004, p.751). In addition, Basel II requires that the bank should have clear and effective policies, procedures, and information systems to monitor compliance with … (Basel Committee, 2004, p.496), that each supervisor will develop detailed review procedures to ensure that banks' systems and controls are adequate to serve … (Basel Committee, 2004, p.6 & p.389), and that management must also ensure, on an ongoing basis, that the rating system is operating properly (Basel Committee, 2004, p.439) in different sections.

However, the methodologies, frameworks, or standards to be referred to as baseline during the supervisory review process on the effectiveness of the above mentioned systems have not been discussed in Basel II. Basel II and other regulations such as Sarbanes-Oxley, Law for Security Exchange Commission (SEC) in the USA, and European Directives do not prescribe actual technologies to use for compliance. Instead, most companies adopt internal control frameworks as models of best practice for compliance where the most common element of all regulations is a strong set of internal controls (Davidson, 2006).

On the other hand, the Information Technology Governance Institute (ITGI) published a draft document entitled Information Technology (IT) Control Objectives for Basel II on 9 May 2007 (2007b). ITGI (2007b) is taking the proactive step of addressing risk in financial service organizations considering that information risk and information technology have become decisive factors in shaping modern business, and many financial service organizations have undergone a fundamental transformation in terms of IT infrastructures, applications, and IT related internal controls. Since IT related

components such as applications, infrastructure elements and controls are all defined as parts of operational risk, ITGI (2007b) maps Basel II principles for operational risk against information technology risk. Therefore, ITGI (2007b) defines a set of ten guiding principles for information risk management, where these guiding principles correspond to the principles of ORM as set down in Basel II.

However, ITGI (2007b) refers only to the Control Objectives for Information and related Technology (CobiT) framework at the sub-domain level. Therefore, the aim of this paper is to assess whether IT Governance frameworks and standards (information control models) are appropriate at the control objective level for controlling the operational risks, and to integrate and harmonize them in order to project an aggregated IT checklist for ORM. In the thesis, the control objectives in information control models (ICMs) have been evaluated and mapped to the operational risk categories in Basel II, rather than bridging the Basel II principles and CobiT principles, so that the ICMs can be compared against the Basel II requirements' fulfillment.

For such an assessment, CobiT, Information Technology Infrastructure Library (ITIL), BS7799, ISO27001, and Committee of Sponsoring Organizations (COSO) have been assessed regarding the Basel II requirements related to ORM. In order to be able to propose a sophisticated IT checklist, the following sections discuss the various definitions of risk, control, operational risk, risk management and measurement, and ORM, in the lights of Basel II ORM requirements and other US and European regulations. Then, many ICMs in the literature are listed and some proposed risk management models referring to these ICMs are evaluated. Basel II operational risk categories and control objectives in the ICMs are mapped, and the mappings are

evaluated by a focus group. Lastly, the aggregated IT checklist for ORM is proposed, which is a best practices approach based on CobiT and structured on COSO.

CHAPTER TWO

BACKGROUND

Definition of Risk

The term risk is used universally, but different audiences often attach slightly different meanings to it (Kloman, 1990). Although there are many variations in how risk is defined, the following definition succinctly captures its essence: risk is the possibility of suffering loss (Dorofee, 1996). This definition includes two key aspects of risk: (1) some loss must be possible and (2) there must be uncertainty associated with that loss.

Thus, risk is subdivided into two types: speculative risks and hazard risks (Young & Tippins, 2001). With speculative risk, you can realize a gain, improving your current situation relative to the status quo. At the same time, you have the potential to experience a loss. In contrast, hazard risk only has potential losses associated with it and provides no opportunity to improve the current situation. Thus, Young & Tippins (2001) classify a risk as speculative or hazard based on its type, but upon the context in which it is viewed. Figure 1 illustrates the differences between these two categories.

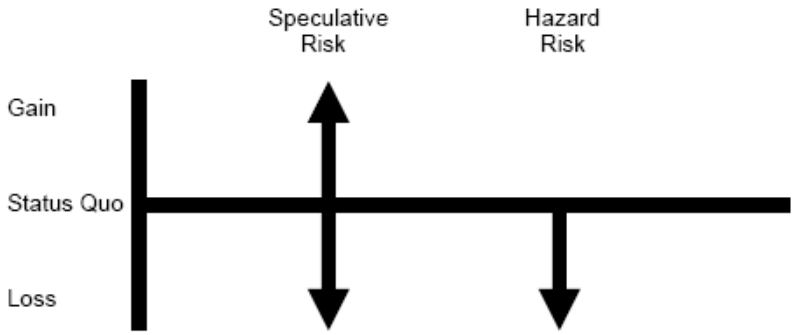

Figure 1: Speculative and hazard risks

Shortreed, Hicks & Craig (2003) define risk as the combination of the probability of an event and its consequences. However, Marshall (2001) associates risk with change by defining risk as the potential for events or ongoing trends to cause future losses of fluctuations in future income. Thornhill (1990) defines risk as a measure of the possibility or deviation from the expected by listing some elements: (1) Possibility of loss or exposure to loss. (2) Probability or chance of loss. (3) Peril which may cause loss. (4) Hazard or condition, which increases the likely frequency or severity of loss. (5) Property or person exposed to loss. (6) Potential dollar amount of loss. (7) Variations in actual losses. (8) Probability that actual losses will vary from expected losses. (9) Psychological uncertainty concerning loss.

All forms of risk comprise common elements (Alberts, 2006). Figure 2 presents these four basic components of risk as: (1) context, (2) action, (3) conditions, and (4) consequence. Context is the background, situation, or environment in which risk is being viewed and defines which actions and conditions are relevant to that situation. The action is the act or occurrence that triggers risk. Whereas the action is the active component of risk, conditions constitute risk's passive element. They are defined as the

current state or the set of circumstances that can lead to risk. Conditions, when combined with a specific triggering action, can produce a set of consequences, or outcomes. Consequences, the final element of risk, are the potential results or effects of an action in combination with a specific condition(s).

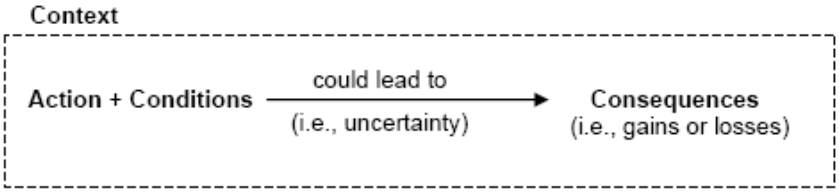

Figure 2: The four elements of risk

Categorization of Risk

There are various categorizations of risk, according to different point of views. Several risk categorizations have been discussed as follows.

Smith, Mc Keen & Staples (2001) categorize the risk concept under financial, technology, security, information, people, business process, management, and external risk classes. Filipovic & Rost (2006) comprise these classes into market, credit, insurance, operational, intra-group risk classes. However, the most known risk categorization is done by Group of Thirty (1993), referred by King (1998), Marshall (2001), and Brag & Wedefelt (2004), and regulated by Basel Committee (2004): market, credit, and operational risk. On the other hand, Carey & Stulz (2005) remodel this categorization as follows: market, credit, and operational; liquidity, strategic, and

business risk; model risk and systemic risk. Baki, Rajczy & Temesvari (2004) present a more detailed and sophisticated risk categorization, as shown in Table 1.

Table 1: An Approach for Risk Categorization

Risk Class	Risk Category	Risk Type
Financial	Credit	Counterparty
		Obligor
		Supplier
		Settlement
	Market	Interest Rate
		Currency
		Equity
		Commodity
		Behavioral
	Liquidity	Hedging
		Funding
		Cash Management
Business	Management	Reporting
		Monitoring
		Organizational
		Planning
	Strategic	Research & Development
		Product Design
		Market Dynamics
		Market Structure
		Business Relationships
		Economic
		Reputational
Operational	People	Interpersonal Relationships
	Process	Compliance Breakdown
		Control Breakdown
	System	Hardware
		Software
		Telecommunications
		Networks
	External	Catastrophic/Event
		Client/Counterparty/Vendor
		Security Breach
		Supervisory
		Systems

Finally, Aktolun (2002) lists all risk types, risk categories, and risk classes, and the relationships among them in Table 2.

Table 2: An Approach for Risk Classification

Risk Class	Risk Category	Risk Type
Strategic	Stakeholder	Shareholder
		Business Partner
		Customer
		Government
		Supplier
	Governance	Ethics
		Strategic Planning
		Resource Allocation
		Corporate Monitoring
		Reputation
	Market	Competition
		Market Dynamics
		Country
		Economic
		Transaction
Operational	Process	Support Processes
		Production & Delivery
		Marketing & Selling
		New Product / Service Development
	Physical Asset	Plant, Property, etc.
		Other Tangibles
	People & Culture	Learning Organization
		Human Resources
	Legal	Legislative & Regulatory
		Contract
		Liability
Information	Systems	Hardware
		Software
		Networks
	Information Management	Planning & Development
		Operations
		Organization & Monitoring
	Intellectual Property	Intangible Assets
		Knowledge Management
		Information
Financial	Market	Commodity
		Interest Rate
		Foreign Exchange
	Liquidity & Credit	Collectibles

		Cash Management
		Hedging
		Funding
	Reporting	Tax
		Accounting
		Regulatory & Compliance
	Capital	Equity
		Debt

Definition of Operational Risk

Managers in every organization deal with risk on many levels. Upper management focuses on the speculative nature of risk. Management balances the risk of investing organizational capital against the potential return on that investment and strategically manages risk across the organization's portfolio of activities and investments. However, at the operational levels of an organization, staff and management focus on managing a form of hazard risk called operational risk. As staff and management execute work processes, operational risks begin to emerge. The deficiencies inherent in processes can lead to inefficiencies and problems during operations, which can adversely affect the organization's chances for success.

There is no universally accepted definition of the term operational risk but there is some consensus among practitioners that operational risk is produced because of a failure or breakdown in operational processes (Blacker, 1998). The first definitions were mostly based on an exclusion principle, such as every type of non-quantifiable risk, or all risks but market and credit risk (Mürmann & Öktem, 2002). King (2001) defines operational risk as the risk not related to the way a firm finances its business, but rather to the way a firm operates its business. He also offers an alternative definition: operational risk is a measure of the link between a firm's business activities and the

variation in its business results. When the Bankers Trust began its study of operational risks in the early nineties, their definition of operational risks was more or less everything that is not market or credit risk (Marshall, 2001 & Hoffman, 2002). They decided to define some risk classes as follows:

- People Risk: the risk of loss caused intentionally or unintentionally by an employee (e.g. employee error or employee misdeed) or involving employees such as in employment disputes.
- Relationship Risk: Non-proprietary losses of a firm generated through the relationship or contract that a firm has with its clients, shareholders, third parties, or regulators
- Technology and Processing Risk: The risk of loss by failure, breakdown or other disruption in technology and/or processing. It also includes loss from the piracy or theft of data or information and loss from technology that fails to meet its intended business needs.
- Physical Risk: The risk of loss through damage to the firm's properties or loss of physical property or assets for which the firm is responsible.
- Other External Risk: The risk of loss caused by the actions of external parties such as in the perpetration of fraud, or in the case of regulators the promulgation of change that would alter the firm's ability to continue operating in certain markets.

Loewenton (2003) categorizes these factors as people, systems, processes, and external reasons as Crouhy, Galai &Mark (2000) classify them under people, process (including

model, transaction, and operational control), and technology risk. Saunders (2000) advocates that the internal sources of the operational risk are employees, technology, customer relationships and capital assets destruction, as the external sources are mainly fraud and natural disasters. Culp (2001) notes that the operational risk examples in the data entry form of the British Banker's Association Operational Risk and Loss Database include failed securities trades, settlement errors in funds transfers, stolen or damaged physical assets, damages awarded in court proceedings, penalties and fines assessed by member associations or regulators, irrecoverable or erroneous funds and asset transfers, unbudgeted personnel costs, and negligence or fraud. These examples include legal risk but exclude reputational and strategic risk (Harris, 2002a) because they are so difficult to quantify and since the focus of the Basel Committee is so much on the measurement side.

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events, in an industry study performed by the British Bankers' Association, the International Swaps and Derivatives Association, Risk Management Association, and PricewaterhouseCoopers in 1999 (BBA, ISDA, RMA & PwC, 1999), as affirmed in Basel II (Basel Committee, 2004) and referred by Netter & Poulsen (2005). Beyond the rules and the modeling requirements for measuring the regulatory capital required to cover operational risk properly, the Basel Committee pays particular attention to the management of this risk by illustrating this concern in the document entitled Sound Practices for the Management and Supervision of Operational Risk (Basel Committee, 2003a and Chapelle, 2005b).

In addition, BRSA (2001) describes operational risk as the risk of loss arising from errors and omissions caused by breakdowns in the internal controls of the bank, the

failure of the bank management and personnel to perform in a timely manner, or mistakes made by the bank management, or breakdowns and failures in the IT system, and events such as a major earthquake, major fire or flood. As seen in the definition, the operational risk is detailed by BRSA considering the possible effects of IT on the business operations and the trigger effect of the operational risk on other risks such as business risks. BRSA (2006a) lists examples such as AT&T's a main switch problem in 1998 where many credit cards were out of function for over eighteen hours, and Imar Bank's fraudulent double booking system in 2003, for the operational failures and frauds based on IT. BRSA (2006b) has also published the Regulation on Information Systems Assurance in the Banks for the assurance of the information systems. The regulation refers (BRSA, 2006b, p.19) to the Control Objectives for Information and related Technology (CobiT) framework while assuring the IT infrastructure of the banks, and requires that the periodic IT audits including the IT based applications controls within the banking business processes are performed beginning from 2007.

The definition of operational risk in Basel II focuses on risk stemming from the execution of work process. However, it does not account for a second, equally important aspect of risk that can occur during operations: the risk associated with the expected outcome of a process, e.g. mission risk. As a result, Alberts (2006) defines a new form of risk called mission risk. His proposed definition for mission risk is the possibility that a mission might not be successfully achieved. In addition, the mission of a work process defines the context in which operational risk is viewed.

Kuritzkes (2002) suggests that operational risk is a non-financial risk that has three sources. The first is internal risk such as risk of rogue traders. The second is external event risk, which is an uncontrollable external event such as a terrorist attack or

weather destruction. The third is business event risk, which captures many things such as price wars or stock market downturn. Kuritzkes (2002) argues that business risk is the most important but is ignored in the Basel II since minimum capital requirement is calculated over credit, market and operational risk (Basel Committee, 2004).

Figure 3 illustrates how the four elements of risk are translated to operational risk and shows the relationships between controls and triggers, vulnerabilities, and impacts (Alberts, 2006). The trigger is the act or event that, when combined with existing vulnerabilities, leads to a range of potential losses. Vulnerabilities are flaws or weaknesses that expose the process to those losses; impacts define the potential losses resulting from a realized risk.

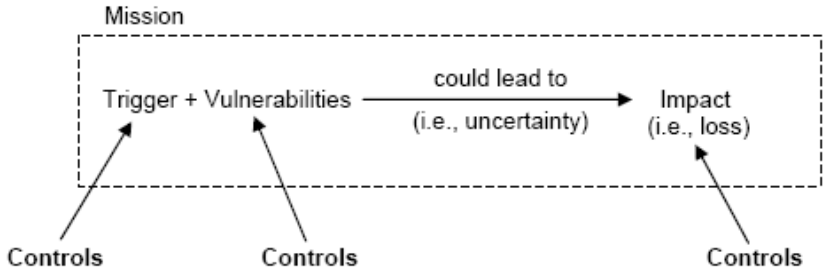

Figure 3: Operational risk elements and controls

Alberts (2006) factors one additional type of condition into the equation for operational risk: controls. Controls in this mission are the circumstances that propel a process toward fulfilling its mission. They include the policies, procedures, practices, conditions, and organizational structures designed to provide reasonable assurance that a mission will be achieved and that undesired events will be prevented, detected, and corrected (ITGI, 2005). Preventive controls attempt to keep deviations from occurring in the first

place, detective controls attempt to detect deviations when they occur, so that necessary actions can be taken in time, and corrective controls actually fix deviations (Panko, 2006).

Moreover, controls are divided into three types according to their scope: company level controls, general controls, and application controls, as shown in Figure 4 (ASOSAI, 2003 & Perry, 2004).

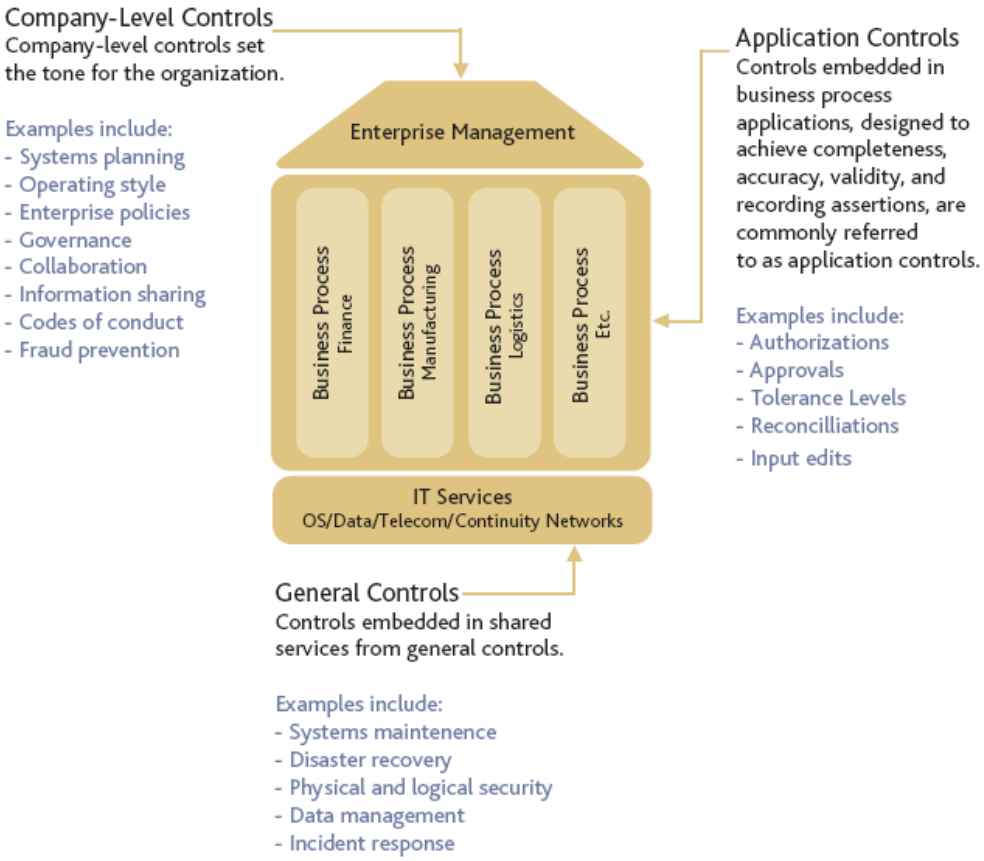

Figure 4: Control framework in an enterprise

ITGI (2004 & 2006b) adds new examples to each category: strategies and plans, policies and procedures, risk assessment activities, training and education, quality assurance, and

internal audit for company level controls; validity, completeness, accuracy, existence, presentation and disclosure, and segregation of duties for application controls; and program development, program changes, computer operations, access to programs and data for general controls. Controls can help reduce risk by eliminating a triggering event, monitoring for the occurrence of a trigger and implementing contingency plans when appropriate, reducing vulnerability, and reducing potential impacts. ITGI (200b) also refers to the Public Company Accounting Oversight Board (PCAOB), describing IT general controls as having a pervasive effect over all internal controls.

Triggers and vulnerabilities are classified as threats by Alberts (2006). A threat is a circumstance or event that produces risk (Alberts & Dorofee, 2005), comprises a trigger and one or more vulnerabilities, because together these elements define the circumstances that create the potential for harm or loss. Sources of operational risk build on the concept of threat by examining the five categories of threat that produce operational risk. Moreover, some people are prone to confusing operational risks with problems and often view them as interchangeable (Alberts & Dorofee, 2005). However, operational risk looks into the future, focusing on problems and failures that have not yet occurred, while a problem describes a situation that is presently taking place.

Past research at the Software Engineering Institute (SEI) examined operational risk in various settings, including software development (Dorofee et al., 1996 and Williams et al., 1999), system acquisition (Gallagher, 1999), and operational security (Alberts & Dorofee, 2002). SEI's research in these areas shows similarities and patterns among the types of threats, sources of operational risks that lead to operational risk. SEI research examines these domains to identify a common structure for classifying sources of operational risk (Alberts & Dorofee, 2005). The key to identifying this common

structure is to decompose a work process into its core elements. A work process is a collection of interrelated work tasks that achieves a specific result and its mission defines the set of the objectives pursued when executing that process (Sharp & Mc Dermott, 2001). There are two structural elements in a work process: mission and process design, and there are three operational elements: activity management, operational environment, and event management.

Table 3: Elements of Operational Threats

Threat Category	Trigger	Vulnerability
Mission Threat	Process execution	A fundamental flaw, or weakness, in the purpose and scope of a work process
Design Threat	Process execution	An inherent weakness in the layout of a work process
Activity Threat	Process execution	A flaw, or weaknesses, arising from the manner in which activities are managed and performed
Environment Threat	Process execution	An inherent constraint, weakness, or flaw in the overarching operational environment in which a process is conducted
Event Threat	Event	Specific vulnerabilities that, when combined with the triggering event, place a mission at risk

The five basic categories of operational threat uniquely map the five work process elements featured previously as discussed by Alberts & Dorofee (2005) by referring to Alberts & Dorofee (2002), Carr et al. (1993), Charette (1989) and Haimes (2004). Table 3 highlights the trigger and vulnerability associated with each category of threat. The table explicitly highlights the fundamental difference between event threats and the other four categories. Whereas an event threat is triggered by an unpredictable occurrence, threats from the other four categories are triggered whenever a work process is executed; no external trigger or occurrence is needed to produce risk.

Of the five categories of threat, event threats stand out as being fundamentally different from the others. The operational risk produced by an event threat is called extrinsic risk because its underlying trigger (i.e., the occurrence of an event) occurs outside of expected or predictable operational conditions. By contrast, threats from the other four categories (mission, design, activity, and environment) do not require an external trigger to produce operational risk. The risk generated by these four categories is called intrinsic risk because it is an inherent part of process execution. The characteristics of intrinsic risk are quite different from those of extrinsic risk (Alberts & Dorofee, 2005). For example, intrinsic risks are often more likely to occur than extrinsic risks because the stimulus needed to produce intrinsic risks (i.e., process execution) is always present. In addition, while extrinsic risk often produces catastrophic consequences, experience shows that intrinsic risks can cause a variety of impacts, ranging from negligible to very high. Catastrophic impacts triggered by a specific source of intrinsic risk, although possible, are rare.

Operational Risk Management

The attention has shifted towards the risk management of operational risk because events resulting from operational risk can have a devastating impact on the operations of banks. Famous cases are Barings' insolvency and the Allied Irish Banks' loss of 750 million dollars due to rogue trading, the 2 billion dollars settlement of the class action lawsuit against Prudential Insurance due to fraudulent sales practices for over 13 years (Mürmann & Öktem, 2002).

Thus, operational risk has become an important part of financial institution risk management efforts partly because it was highlighted by the Basel Committee and Section 404 of Sarbanes-Oxley, and partly because of the disruptions associated with the September 11 attacks. Though some still doubt whether it is material or even can be measured, financial institutions increasingly allocate capital to operational risk. For instance, a survey by Risk Waters Group and SAS found that one of five financial companies still does not have a risk management program, yet 90% of these companies loose more than 10 million dollars a year because of poor risk control practices (Marshall & Heffes, 2003). In addition, a survey by Oliver Wyman and Company of ten large international banks found that they allocate 53% of their economic capital to credit risk, 21% to market risk and asset-liability rate risks, and 26% to operational and other risks (Carey & Stulz, 2005).

Hiwatashi (2002) argues that banks have already begun to consider operational risk because of advances in information technology, deregulation, and increased international competition. Similarly, the increase in the number of large mergers and acquisitions, where the combined firm must integrate the systems of the merged firms, can lead to increased operational risk. Cumming & Hirtle (2001) discuss the analysis of comprehensive risk management in financial institutions. A conference at the Federal Reserve Bank of Boston (2001) provides several examples of the differing approaches to operational risk management that have been suggested by various banks and consulting firms. Cagan (2001), and Nash, Nakada & Johnston (2002) offer specific suggestions for institutions preparing for the implementation of Basel II.

Hiwatashi (2002) reports several reasons why banks try to measure operational risk. Firstly, by measuring operational risk banks are able to develop objective criteria in

analyzing the adequacy of internal risk control measures. Secondly, banks have long established risk management systems to analyze whether they have adequate economic capital to deal with market and credit risk. Harris (2002a) notes that proper management can improve bottom line earnings by reducing exposure to low frequency but high impact losses. In addition, proper risk management can reduce insurance premiums and lower capital requirements, especially when Basel II is fully implemented. Donnelly (2001) takes this final point further and argues that proper operational risk management needs to provide audit committee members with information on the methodology used in risk assessment, identification of issues, and resolution and tracking mechanisms. Rosengren (2002) also argues that financial organizations should manage operational risk because of the significant potential costs of operational risk losses. King (2001) discusses some examples (and provides data on 89 cases) where financial service firms suffered large losses because managers did not monitor and control the risk of operational processes. In addition, Buchanan, Arnold & Nail (2002) analyze the corporate governance failures that led to the collapse of Australia's second largest insurer, and Buchanan & Netter (2002) analyze the money laundering scandal of the Bank of New York.

Thornhill (1990) defines risk management as a management discipline whose goal is to protect the assets and profits of an organization by reducing the potential for loss before it occurs, and financing through insurance and other means, potential exposures to catastrophic loss. Loewenton (2003) lists the building blocks of ORM as shown in Figure 5.

Figure 5: The building blocks for operational risk management

Loewenton (2003) offers alternatives for ORM, such as transferring the risks to a third party company or appropriate insurance, mitigating the risks by reducing the likelihood of or the impact, accepting the risks within a defined risk tolerance, or eliminating the risks. In addition, Information Systems and Control Association (ISACA) (2006) notes that effective risk management begins with a clear understanding of the organization's appetite for risk. Having defined risk appetite, and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Dependent on the type of risk and its significance to business, management and the board may choose to:

- Avoid, i.e. where feasible choosing not to implement certain activities and processes that would incur greater risk.
- Mitigate, i.e. define and implement controls to protect the IT infrastructure.
- Transfer, i.e. share risk with partners or transfer to insurance coverage.
- Accept, i.e. formally acknowledge the existence of the risk and monitor it.
- Eliminate, i.e. where possible, remove the source of the risk.

Mitigating operational risk requires an investment of resources; therefore, it is important to understand exactly how much you should spend in order to keep risk at an acceptable level. Operational risk tolerance is the maximum overall exposure to operational risk that will be accepted, given the costs and benefits involved. Alberts & Dorofee (2005) illustrate the concept of operational risk tolerance in Operational Risk Tolerance Matrix as shown in Figure 6. Before any mitigation action is taken, the operational risk in the figure must exceed management's tolerance. Management must be willing to invest resources to reduce it.

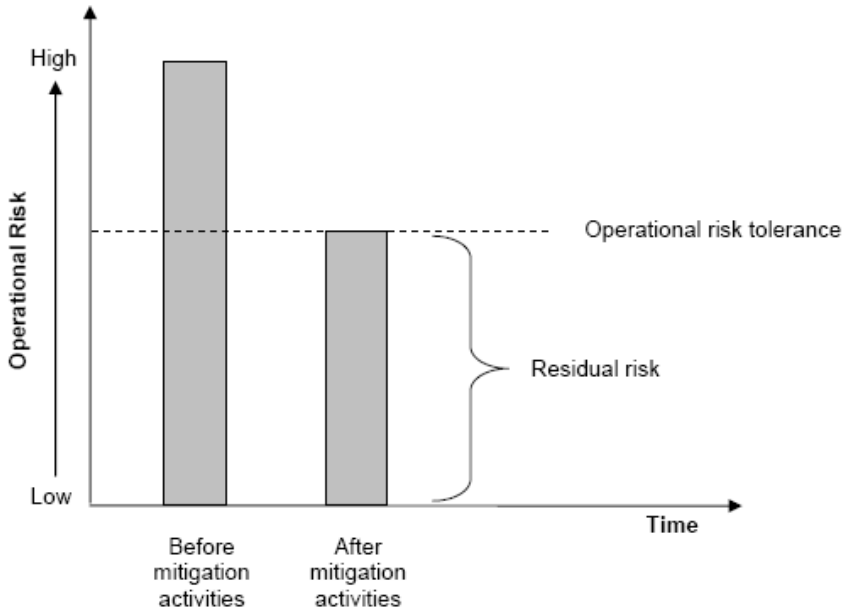

Figure 6: Operational risk tolerance

Unless all IT systems or processes pose a high risk to the financial statements, not all IT systems or processes need to be included or evaluated to the same extent. In performing

a risk assessment, consideration needs to be given to inherent risk rather than residual risk, which is the risk left over after considering the impact of controls (ITGI, 2006b).

Managers are finding it extraordinarily difficult to deal with the degree of operational risk confronting them on a daily basis. Although many factors contribute to this problem, two are especially influential. First, some risks are not communicated effectively to people who are in the best position to manage them. The second reason is the inability to manage process and technological complexity effectively, making it difficult to establish accurate risk profiles.

Keeping operational risk within tolerance minimizes problems during operations and enables the management to handle any problems that occur more easily, while directing most of its effort toward achieving the mission at hand. Three fundamental tactics for achieving mission assurance are also illustrated in Mission Assurance Strategy in Figure 7 by Alberts & Dorofee (2005).

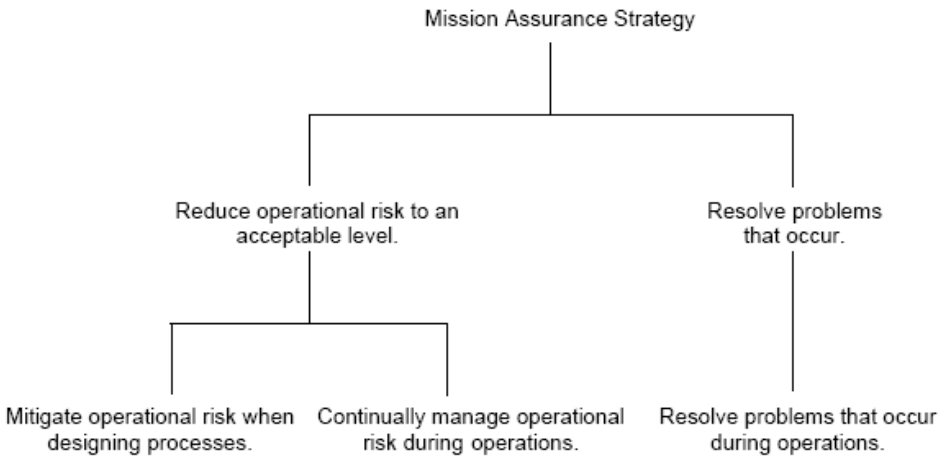

Figure 7: Mission assurance strategy

Operational Risk Measurement

Risk measurement methodologies emphasize the importance of internal loss data, quantification and measurement is only possible if we attach loss estimates to particular risk events and a probability of such an event to occur. The first step into quantifying risks is to categorize different types of operational risks according to the existing categorizations. Then one method for quantifying risks is applied. There are two ways of measuring operational risks (Hiwatashi, 2002):

- Top down approaches: estimating on a macro basis without identifying events or causes of losses. This type of approach calculates a capital charge at firm level.
- Bottom up approaches: measuring based on identified events (using a loss event database) and per business line and the calculation is done at that level.
    - Statistical measurement: the maximum loss of operational risk is measured based on events and on frequency and severity using an analytical solution
    - Scenario analysis: losses are estimated based on scenario (with reference to external data and events which occurred in other banks or to variation of data in the internal loss database)

Operational risk encompasses events with very different frequencies and possibly patterns of occurrence and severities. As a first step in determining the applicability of statistical analysis, it seems appropriate to first qualitatively categorize potential

incidents into a frequency severity matrix based on scorings or possibility (Loewenton, 2003). Figure 8 presents a frequency severity matrix based on scorings.

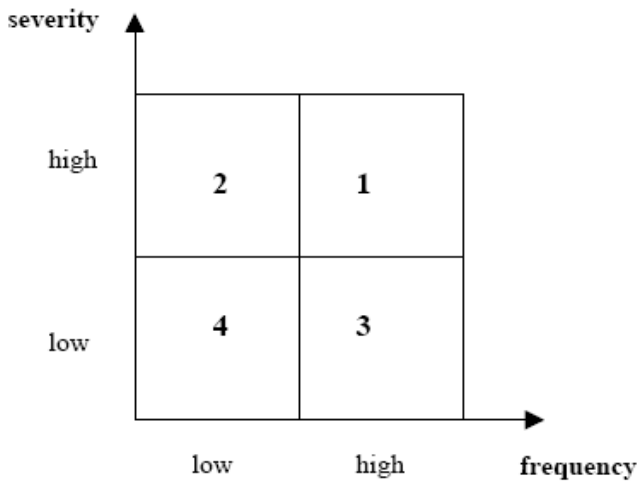

Figure 8: Frequency severity matrix based on scorings

This frequency severity matrix additionally gives first guidance in prioritization of events. Risk managers should pay great attention to high frequency & high severity (area 1) and relatively less attention to low frequency & low severity (area 4) events. Unfortunately, the low frequency of these events implies very few data points. The estimation of probabilities and loss distribution will thus only produce highly unreliable results. Risk management decisions based solely on those statistical outcomes may lead to consequences that are as devastating as the ones to which the analysis has been applied. The advantage of high frequency events is the possibility of creating large databases on which statistical analysis can be accurately based. It is the concern of risk managers that the qualitative matrix above is actually not accurate or stable and that low severity events actually turn out to be high severity events.

Loewenton (2003) refers to the monograph by Embrechts, Klueppelberg & Mikosch (1997) and the references therein for a concise overview on the extreme value theory. A major drawback of that approach, however, is that risk measures (Herring, 2002) such as the Value at Risk (VaR) or Risk Adjusted Return of Capital (RAROC) depending on the overall loss distribution are very sensitive to the chosen threshold level that separates the empirical from the fitted fat-tail distribution in Figure 9. A concept has not been developed yet that defines optimality in terms of the threshold level. Diebold, Schuermann & Stroughair (2000) critically review the applicability of the extreme value theory to risk management.

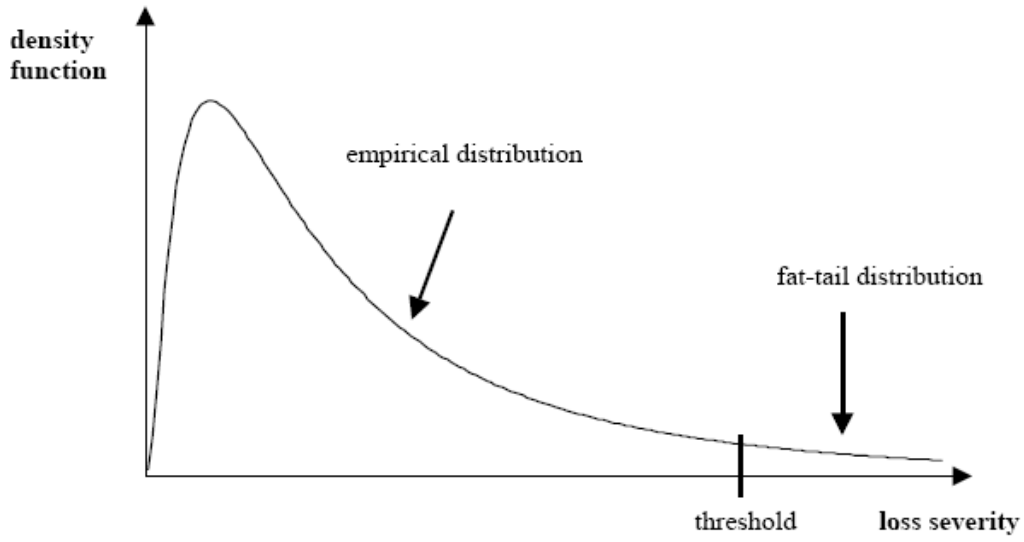

Figure 9: Fat tail distribution

Alexander (2003) states that a risk cannot be measured, a risk is not like a length of hosepipe than can be checked with a measuring tape. A risk is about the future, it can only be assessed by using some model, some hypothetical representation of possible

future realization, it is presumptuous to imagine that operational risks will one day be measured with accuracy; it is much more realistic to believe that there will be a fine mixture of assessment, estimation and measurement.

Harris (2002a) provides a basic overview of what advanced financial organizations are doing to address operational risk that summarizes the implementation of operational risk management. He identifies this pattern: recognizing operational risk as a separate discipline, restructuring the organizational hierarchy, defining a management process, creating measurement tools, developing monitoring systems. Harris (2002b) also outlines the role of an operational risk manager in a firm. The role includes: document risk management policy, ensure senior management buys into policy, establish reporting and metrics, promote capital data management systems, develop loss tracking methods, and map to business line by proxy (such as net income). Alexander (2003) presents some statistical models for operational loss, he discusses the loss distribution approach, and Cruz (2002) describes a variety of statistical techniques to model operational risks and stochastic and causal models that can be used to measure and manage risks. In a Chartis (2006) research document, ORM systems are presented as shown in Figure 10.

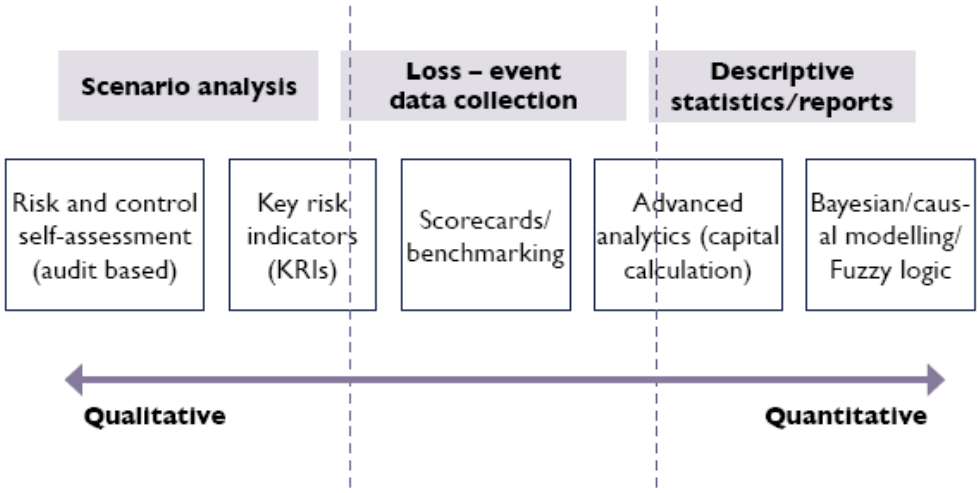

Figure 10: Spectrum for operational risk management systems

Risk Management in Practice

Chapelle (2005b) presents his approach to the structure of risk management in four dimensions, from the most static one to the most proactive one, each of them being an input for the following. The four dimensions are the following:

1. Incident Reporting: Static analysis. It gives a cartography of past events, their nature and their cause.
2. Dashboard: Dynamic analysis. It describes the evolution of operational events by activity or by department, providing a dynamic representation of the losses.
3. Key Risks Indicators (KRIs) / Key Performance Indicators (KPIs): Benchmarking analysis. It allows a comparison of the dashboards to predefined standards and an assessment of the evolution of the risk.

4. Risk and Control Self Assessment (RCSA): Proactive analysis. It provides a prospective view of the potential risk based on the collection of information by experts in the field.

Near-Miss Concept

Mürmann & Öktem (2002) propose the risk management concept Near-Miss which is used in the chemical, health and airline industries. They consider Near-Misses as weak signals, some of which contain a genetic signature of a serious adverse effect. Analogously, major operational losses in the banking industry have their predecessor in the form of small abnormalities that do not necessarily cause any losses. Since Near-Misses provide insight into potential major adverse conditions and business disruptions, addressing Near-Misses timely and properly discourages major problems from flourishing (Jones, Kirchsteiger & Bjerke, 1999). Near-Misses are defined in a variety of ways by different authors (Barach & Small, 2000, and Phimister et al, 2001b). While some definitions are very focused and based on the extent of the potential negative consequences, such as that Near-Miss is an undesired event or sequence of events with the potential to cause serious damage, Mürmann & Öktem (2002) prefer the following definition: Near-Miss is an event, a sequence of events, or an observation of unusual occurrences that possesses the potential of improving a system's operability by reducing the risk of upsets, some of which could eventually cause serious damage. Along the lines of the Near-Miss system that has been developed for chemical process industries by Phimister et al. (2001a), Mürmann & Öktem (2002) propose the following eight-step ORM process for financial institutions:

1. Identification (recognition) of a Near-Miss.
2. Disclosure (reporting) of the identified information/incident.
3. Prioritization and Classification of the information for future actions.
4. Distribution of the right level of information to the proper channels.
5. Analyzing Causes of the problem.
6. Identifying Solutions (remedial actions).
7. Dissemination of actions to the implementers and (optional) general information to a larger group for their knowledge.
8. Resolution (wrap-up) of all open actions and completion of reports.

This structure of incidents is commonly accepted in process industries and represented by the safety pyramid (Bird & Germain, 1996) in Figure 11. Near-Misses represent the lower portion of the pyramid. Therefore, the Near-Miss system fits into the total quality management principles for operational risk as mentioned in Marshall (2001) and Hoffman (2002).

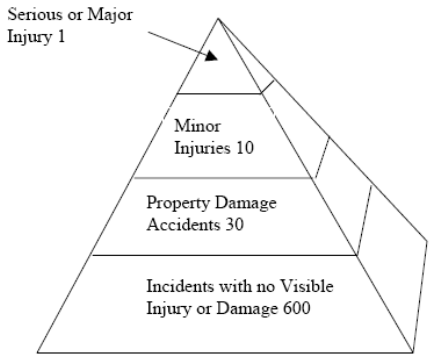

Figure 11: Safety pyramid

Other Measurement Methods

The idea of trying to apply operational research methods to optimize operational risks arose upon the realization that operational research is usually aimed at optimizing something. Loewenton's (2003) proposal is to use graph theory with a set of nodes and a set of directed arcs, each arc connecting one or more nodes together. On each node and on each edge, a value (a weight) indicates the probability of failure (of the process represented). The idea behind this is to calculate a lower bound for each workflow, which would indicate what the minimum risk that each activity bears is. Then it is a matter of strategy to determine how much more the bank is accepting to put at risk for each business activity.

The Federal Reserve Bank of Chicago has developed eight components for examiners to use in evaluating operational risk (Kvistad & Donnelly, 2001). Each of these indicates a potential for operational risk losses. The first is growth and consolidation, a rapidly growing bank, or recently consolidated banks that have a greater potential for operational risk losses. The second is the quality of the information systems. The third is the quality, training, and morale of the employees. The fourth is the transaction volume and complexity of the transactions of the bank. The fifth is the bank offering new products and services. The next is the ripple effect, what would be the indirect effect of an operational disruption. The seventh is the facilities and geographical dispersion of the bank. The final component of operational risk is electronic delivery, with its complexity and security challenges.

Regulation on Operational Risk Management

In response to the problems related to the risk management methods mentioned above, the banking industry called for regulatory bodies to address operational risk. Therefore, regulators set out a framework on capital requirements, Basel Accord, involving methods of risk quantification. Beginning with the initial Basel Accord in 1988, known as Basel I, based on a model to measure the capital, risk was based across exposure groups and not the individual elements of credit worthiness within these groups, by the Basel Committee on Banking Supervision (the Basel Committee) structured under the Bank for International Settlements (BIS) which is the world's oldest international financial institution (Basel Committee, 2002c). Various market developments since 1988 in terms of product innovation, deal structuring, risk mitigation techniques and the use of increasingly sophisticated derivative instruments led to a need for a more sophisticated way of allocating capital to risks. Therefore, BIS published a revised Basel Accord in June 2004, known as Basel II.

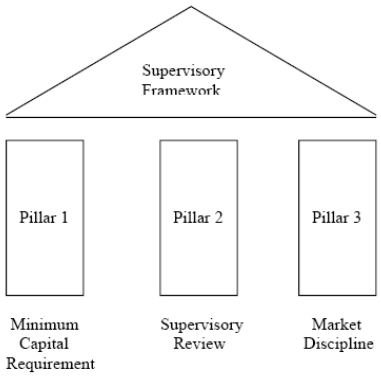

Figure 12: The three pillars of Basel II

The fundamental objective of the Basel Committee in revising the 1988 Basel Accord and publishing the revised Basel II has been defined as developing a framework that would further strengthen the soundness and stability of the international banking system while maintaining sufficient consistency that capital adequacy regulation will not be a significant source of competitive inequality among internationally active banks (Basel Committee, 2004, p.4). Since the purpose of Basel II was to enhance the way banks cover and manage their risks, it is based on three pillars: minimum capital requirements, supervisory review, and market discipline (Basel Committee, 2002a, 2002b, 2004). Figure 12 from Cruz (2002) shows how crucial the three pillars are for maintaining the edifice of Basel II.

Basel II

The first pillar, presented as the minimum capital requirements, requires the calculation of the total minimum capital requirements for credit, market, and operational risk (Basel Committee, 2004, p.40). Measurement techniques for operational risks remain in an early development stage in most banking and financial institutions. Therefore, until further and better methodologies are proposed, the Basel Committee proposed that operational risk follows three types of approaches for assessing capital against risks (Basel Committee, 2004):

- Basic Indicator Approach (BI): This is the simplest approach. Capital required for operational risk is equal to a percentage (today 15%) of the Gross Income of the institution, under the hypothesis that risk is related to size. Gross income is

the sum of the interest margin, the fee income, and the other revenues. This most simple approach is only available to local banks.

- Standardized Approach (SA): It is a more complex approach based on the Basic Indicator Approach. The capital charge required for operational risk is calculated for each business line (Retail Banking, Investment Banking, Asset Management, etc.). For each business line, the capital required for operational risk is equal to a percentage (between 12% for the least risky business lines such as Retail Banking, Retail Brokerage, Asset Management and 18% for the riskiest ones such as Corporate Finance, Trading and Sales, Payment and Settlement) of the average Gross Income of the last three years. The capital required for operational risk is equal to a percentage with an intermediate level at 15% of gross income for Commercial Banking, Agency Services, etc.
- Advanced Measurement Approach (AMA): An advanced approach where the bank calculates its required capital by incorporating into the calculation its internal loss data, with a confidence interval of 99.9%. This approach requires that the bank aggregate its loss data using the business lines/event types grid provided by the Basel Committee. This sophisticated approach is strongly recommended for banks that are internationally active. In order to adopt the AMA, banks have to comply with numerous quantitative and qualitative criteria regarding their risk management tools, techniques, involvement and expertise in the field of operational risk.

To qualify to use the AMA approach to calculate operational risk capital under Basel II, the Basel Committee (2004, p.665) states that a bank's measurement system must also be capable of supporting an allocation of economic capital for operational risk across business lines in a manner that creates incentives to improve business line operational risk management. This implies a commitment to continuous improvement of ORM, and associated ORM processes, across the organization. In addition, a bank must meet stringent qualitative standards, in summary (Basel Committee, 2004, p.666):

- An independent operational risk management function.
- An operational risk measurement system that is closely integrated into the day-to-day risk management processes of the bank.
- Regular reporting of operational risk exposures to business units, senior management, and the Board, with procedures for appropriate action.
- An operational risk management system that is well documented.
- Regular reviews of the operational risk management processes/systems by internal and/or external auditors.
- Validation of the operational risk measurement system by external auditors and/or supervisory authorities, in particular, making sure that data flows and processes are transparent and accessible. In raising the bar on how ORM systems must be documented, the Basel Committee (2004, p.666) states that it is necessary that auditors and supervisory authorities are in a position to have easy access, whenever they judge it necessary and under appropriate procedures, to the ORM system's specifications and parameters.

The second pillar presented as the supervisory review process (Basel Committee, 2004), requires each bank to have a mechanism to identify and assess their risk and to have a rigorous control environment that will monitor, control and even mitigate the risks. Supervisors should review capital adequacy assessments and should take appropriate measures in case the result is not considered as satisfactory, they should ensure that regulatory capital never falls below a certain limit and if so should take all action to restore the capital charge above this limit.

The third pillar, presented as market discipline (Basel Committee, 2004), requires that the banks should publicly and timely disclose regulatory capital allocation per business line, description of the measurement approach used to calculate capital allocation, detailed information about the process used to manage and control their operational risks (including the organization of its risk management function and its policy for hedging and mitigating risks).

On the other hand, Kane (2001) argues that international regulatory standards are inferior to competition among national regulatory systems, especially in strengthening the banking systems in developing countries. Petrou (2002) notes that regulatory actions can make economic cycles more volatile. Goldstein (2001) is much more positive about the potential for value-increasing international regulatory standards, especially if flexibility is built into the standards and if the international standards do not reach down into all aspects of the financial system. Barth, Caprio & Levine (2001a, 2001b, and 2002), however, empirically examine the relation between regulatory restrictions and bank performance. They find that greater restrictions are associated with higher probability of major banking crises, lower bank efficiency, and have no countervailing positive effects.

There are also some critiques on Basel II, beginning from the proposal of Basel II. Kuritzkes (2002) thinks that BIS or any other regulatory authority cannot come up with any rules for how much capital banks can hold against operational risk since the first line of defense for such risk is internal controls. Mürmann (2002) notes that operational risk is bank specific and thus regulatory capital requirements are not appropriate. ISDA (2000) argues that the capital requirements are unworkable and can lead to distorted actions, such as attempts to avoid control rather than mitigate risk, but stresses the importance of strong supervision and market discipline. Netter & Poulsen (2005) ask several questions which include: (1) What are the key challenges in quantifying operational risks in banks? (2) What will be the requirements for banks to qualify for the AMA in determining capital requirements? (3) To what extent should firms differentiate between regulatory capital requirements and economic capital needs? (4) To what extent can firms integrate the three areas of risk – credit, market and operational? (5) Are there differing bank characteristics that suggest different approaches to risk management? How does a firm determine its best practices relative to its competitors?

In addition to the Basel Accords, the Basel Committee (2003a) published the document entitled Sound Practices for the Management and Supervision of Operational Risk, which describes through a set of ten principles how to manage operational risks efficiently. Loewenton (2003) summarizes these principles as follows:

1. The board of directors should be aware of the major aspects of the bank's operational risks and review the work done regularly.
2. The board of directors should ensure that the operational risk is under internal audit by independent and competent staff.

3. Senior Management should have the responsibility for implementing the operational risk management framework in a coherent and coordinated manner for the entire company.
4. The bank should identify and assess the operational risk in all activities, processes and systems.
5. A process for regularly monitoring operational risk profile and exposure to losses should be implemented.
6. Banks should have policies, processes and procedures to control and mitigate operational risks.
7. Banks should have in place contingency and business continuity plans.
8. Banking supervisors should require banks to have a framework in place for identifying, assessing and monitoring operational risks.
9. Supervisors should conduct regular evaluations of the bank's policies, procedures and practices.
10. Banks should make sufficient public disclosure of their approach to operational risk management.

In addition to Basel II, the European Commission has welcomed the signing by the European Council and the European Parliament of the Capital Requirements Directive (CRD) for credit institutions and investment firms (EU, 2006a). The CRD introduces an updated supervisory framework in the European Union (EU), which reflects the Basel II rules on capital standards agreed at G-10 level since Basel II does not have a regulatory status. Moreover, Statutory Audit Directive (SAD) refers to Sarbanes-Oxley (USC, 2002) and is known as EuroSox (EU, 2006b).

Loss Event Types and Loss Data

Thornhill (1990) details the definition of loss as the incidents that result in direct or indirect economic or monetary loss.

For the purposes of internal ORM, the banks must identify all material operational risk losses consistent with the scope of the definition of operational risk and the loss event including those related to credit risk (Basel Committee, 2004, p.673). In addition, the Basel Committee (2004, p.671) notes that internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and risk management procedures. Therefore, a bank must have documented procedures to assess the on-going relevance of historical loss data, including those situations in which judgment overrides, scaling, or other adjustments may be used, to what extent they may be used and who is authorized to make such decisions. Moreover, the Basel Committee (2004, p.676) notes, in addition to using loss data, whether actual or scenario-based, a bank's firm-wide risk assessment methodology must capture key business environment and internal control factors that can change its operational risk profile. These factors will make a bank's risk assessments more forward-looking, more directly reflect the quality of the bank's control and operating environments, help align capital assessments with risk management objectives, and recognize both improvements and deterioration in operational risk profiles in a more immediate fashion.

Loewenton (2003) argues that collecting data and organizing the database covering the size and frequency of particular loss types is a difficult step in the process of measurement of risks. In order to comply with the AMA, banks are required to have an incident database of minimum three years' history at the Basel II implementation

date. This means that they needed to have started to collect their loss data by January 2004 at the latest.

Therefore, the Basel Committee defined seven loss event types for recording internal loss data as shown in Table 4. This list is not exhaustive and banks are required to work on defining more precisely the type of risks that they are facing. There are also different sources and consortiums to supplement internal data with external data, such as OpVantage, ORX, or the British Bankers Association's GOLD (Loewenton, 2003) and MORE, FIRST, and DIPO (TBB, 2004). However, the difficulties linked to the optimal mix of internal and external data to model the distribution are addressed in Frachot, Georges & Roncalli (2001 and 2002), in Chapelle et al. (2004 and 2005a).

Table 4: Loss Event Types in Basel II

Level 1	Level 2	Definition	Examples
Internal Fraud	Unauthorized activity Theft & Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party	Transactions not reported Unauthorized transaction Mismarking of position Fraud, theft, extortion, embezzlement, robbery, malicious destruction of assets, check kitting, impersonation, insider trading, etc.
External Fraud	Theft & Fraud Systems Security	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations by a third party	Fraud, theft, robbery, , check kitting, forgery Hacking damage, theft of information
Employment Practices & Workplace Safety	Employee Relations Safe Environment Diversity & Discrimination	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events	Compensation, benefit, termination issues Organized labor activity General liability, employee health and safety rules events All discrimination types
Clients, Products & Business	Suitability, Disclosure &	Losses arising from an unintentional or negligent	Fiduciary breaches, guideline violations, suitability/disclosure issues, retail

Practices	Fiduciary Improper Business or Market Practices Product Flaws Selection, Sponsorship & Exposure Advisory Activity	failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements) or from the nature or design of a product	consumer disclosure violations, breach of privacy misuse of confidential information, lender liability Antitrust, improper trade/market practices, market manipulation, insider trading, unlicensed activity, money laundering Product defects, model errors Failure to investigate client per guidelines, exceeding client exposure limits Dispute over performance of advisory activities
Damage to physical Assets	Disaster and other events	Losses arising from loss or damage to physical assets from natural disaster or other events	Natural disaster losses (earthquakes, fire and floods) Human losses from external sources (terrorism, vandalism)
Business Disruption & System Failures	Systems	Losses arising from disruption of business or system failures	Hardware, Software, Telecommunications, Utility outage/disruptions
Execution, Delivery &Process Management	Transaction Capture, Execution & Maintenance Monitoring & Reporting Customer Intake & Documentation Customer/Client Account Management Trade Counterparties Vendors & Suppliers	Losses arising from failed transactions processing or process management, from relations with trade counterparties and vendors	Miscommunication, data entry, maintenance or loading error, missed deadline or responsibility, model/system mis-operation, accounting error/entry error attribution, delivery failure, collateral management failure, reference data maintenance Failed mandatory reporting obligation, inaccurate external report Clients permission missing, legal documents missing/incomplete Unapproved access given to accounts, incorrect clients records, negligent loss or damage of client assets Non-client counterparty mis-performance, misc. non-client counterparty disputes Outsourcing, vendor disputes

A comprehensive analysis of the overall operational risk loss experience in financial institutions was conducted by the Risk Management Group (RMG) of the Basel Committee (RMG, 2002). The RMG published the results of the second quantitative impact study (QIS2) in 2002. QIS2 - Tranche 1 focused on internal capital allocation

data for operational risk and information about other exposure indicators. In QIS2 - Tranche 2, the RMG gathered data on individual operational risk loss examples. The data was collected from thirty banks in eleven countries. The RMG collected the number of loss events and gross loss amounts for eight business lines: (1) corporate finance, (2) trading and sales, (3) retail banking, (4) commercial banking, (5) payment and settlement, (6) agency and custody services, (7) asset management, and (8) retail brokerage. There were 27,371 loss events with a total value of 2.6 billion Euros. Most of the events and the largest Euro value of the losses were in retail banking (67% and 39% of all events and losses respectively) and commercial banking (13% and 23% respectively), which may reflect where the sample firms do most of their business.

The RMG report also compiled results on the distribution of the size of the loss events. Most of the loss events were relatively small, only one percent of the sample was events with losses of one million Euros or more. However, the large loss events dominated the total value of the losses. Events with losses over one million Euros accounted for almost three-fourths of the total losses. The RMG report also reports recovery rates and percent of losses that were recovered, where recovery comes from insurance and other sources.

The RMG reports that there are significant problems with these data but they do show recovery in 12.2% of all events (36.1% of the greatest magnitude loss events), with recovery when it occurs averaging 81.6% of the loss. Table 5 represents the operational risk loss information that the thirty contributing banks were able to supply according to the loss event types defined in Basel II. (Basel Committee, 2004, annex.7).

Table 5: Frequency Severity Matrix for Basel II Loss Event Types

(in percentages)

Loss Event Type	Event Number	Loss Amount
Internal Fraud	2.72	10.66
External Fraud	36.39	20.32
Employment Practices and Workplace Safety	2.71	2.92
Clients, Products & Business Practices	6.39	27.51
Damage to Physical Assets	4.48	3.02
Business Disruption and System Failures	5.32	0.82
Execution, Delivery & Process Management	41.99	34.75

Source: QIS2 Results (RMG, 2002)

Mazıbaş (2005) compounds the operational risk categories defined by Loewenton (2003) and the loss event types categorized by the Basel Committee (2004) under operational risk data classification as follows in Table 6.

Table 6: Operational Risk Data Classification

Loewenton's Operational Risk (Factors)	Basel Committee's Loss Events (Incidents)
Process	Internal Fraud
System	External Fraud
People	Employment Practices and Workplace Safety
External	Clients, Products & Business Practices
	Damage to Physical Assets
	Business Disruption and System Failures
	Execution, Delivery & Process Management

Information Technology Governance

These regulations, frameworks, definitions and attitudes published by USC, BIS, EU, BRSA, and other stakeholders lead us to question whether current ICMs are applicable for controlling the operational risks defined in Basel II. The organizations are increasingly exposed to various operational risks related to the use of IT, e.g. virus attacks, unauthorized access to data, breakdown of infrastructure, system and

infrastructure contingency, and performance problems, since IT is a rapidly changing area that is accompanied by uncertainty and risk.

As the IT environment becomes more dynamic and complex, it is a difficult and frustrating area to manage (Hardy, 2002 & Tyler, 2000). It might thus be expected that IT governance, the corporate governance of IT, would be a significant concern of boards (Musson & Jordan, 2004) since IT is now intrinsic to and pervasive within enterprises (ISACA, 2006). In order to prevent such risks efficiently, the banks are forced to identify, analyze and evaluate potential IT related operational risks, and should implement appropriate IT Governance (Jochum, 2006). Consequently, dependency on IT requires effective IT Governance from management in order to provide a controlled IT framework to the business processes. Thus, IT Governance enables an organization to attain three vital objectives: regulatory and legal compliance, operational excellence, and risk optimization, especially in light of the requirement that US companies must monitor IT Governance as part of their compliance with the provisions of the Sarbanes-Oxley (Hoffmann, 2003).

IT Governance is concerned about IT's delivery of value to the business and mitigation of IT risks (ITGI, 2003), and is considered to be part of corporate governance (Dellit, 2002 & Hamaker, 2003 & Machin, 2002). Under the responsibility of executives and board members, governance activities must flow through various levels of the enterprise (ITGI, 2003). IT Governance focuses on the strategic alignment of using IT to achieve business goals and objectives, and has to provide the organizational structures for the assurance that there are no IT investments in bad projects and that there are adequate IT control mechanisms (Grembergen, 2000) to enable the creation of business value through IT. The importance of IT Governance to corporate governance is

evidenced by an emerging understanding that the most significant IT issues for the near future in both the private and the public sector are not technology-related, but governance-related (Guldentops, 2002).

Organizations can ease their venture into IT Governance, to ensure that the enterprise's IT sustains and extends the organization's strategies and objectives (ITGI, 2005), by leveraging various industry standard frameworks since management's goals and objectives in utilizing the technology to support business processes include confidentiality, integrity, availability, reliability, and compliance with legal and regulatory requirements (ASOSAI, 2003). On the other hand, a survey conducted by ITGI and PricewaterhouseCoopers in 2003 among top management, shows that 42% of the respondents were not considering the implementation of an IT governance solution/framework (ITGI & PwC, 2004). However, the survey conducted in 2005 shows that the share of companies that were not considering implementation was lower than the 2003 results, 36% (ITGI & PwC, 2006).

IT control frameworks set out the best practices for IT actions, processes and monitoring within organizations, and are believed to lead to more effective IT Governance (Warland & Ridley, 2005). Champbell (2003) categorizes over fifty ICMs under control objectives communities, principles communities, capability maturity communities, checklists, risk management frameworks, and taxonomies in his study. Most frameworks provide requisite support materials in the form of roadmaps, guides, templates, libraries, and samples. ICMs covered in his study are presented in a time diagram in Figure 13.

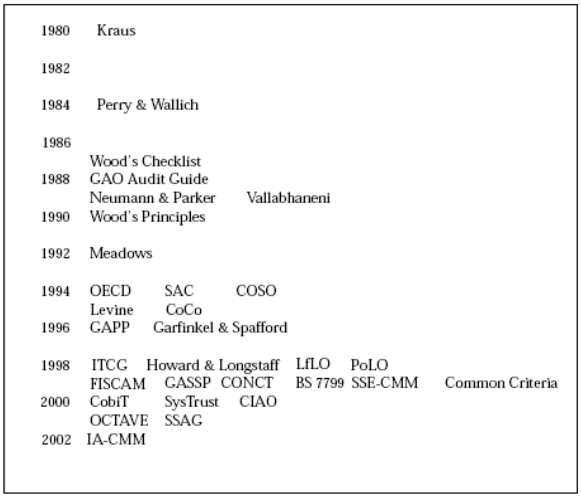

Figure 13: Time diagram

Categorization of Information Control Models

Campbell (2003) categorizes ICMs under the following classes: control objectives community, principle community, capability maturity community, and other models such as proprietary models, checklists, and taxonomies. All these ICMs are influenced by each other as shown in Figure 14.

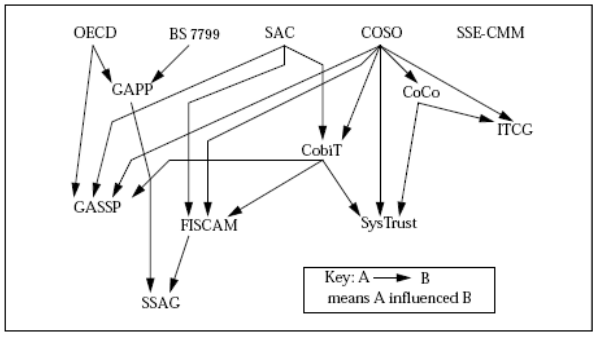

Figure 14: Influence diagram

The control objectives community is based on the concept of control objective, which means a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity (ITGI, 2000). This community has the following members:

- BS7799: Information security management standard produced by the British Standards Institute (BSI)
- ISO27001: Information security management standard produced by the International Organization of Standardization (ISO)
- AS/NZS 4444: Information security management standard produced by the Australian/New Zealand Standard Institutes
- CobiT: Control Objectives for Information and related Technology. IT Governance framework produced by IT Governance Institute (ITGI)
- CoCo: Guidance on Control. Guidance for information assurance produced by the Criteria of Control Board of The Canadian Institute of Chartered Accountants (CICA)
- COSO: Internal Control - Integrated Framework. Enterprise risk management framework generated by the Committee of Sponsoring Organizations of the Treadway Commission
- FISCAM: Federal Information Systems Controls Audit Manual. Manual produced by the Accounting and Information Management Division of the U. S. General Accounting Office
- ITCG: Information Technology Control Guidelines. Guideline developed by the Canadian Institute of Chartered Accountants (CICA)

- SysTrust: AICPA/CICA SysTrust Principles and Criteria for System Reliability. Principle developed by the American Institute of Chartered Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA)

The principles community is based on the notion of principles, such as accountability, awareness, and ethics. Garfinkel & Spafford (1996), Allen (2001), Pipkin (2000), and Wood (2001) expand sets of principles and practices. This community has the following members:

- GAPP: Generally Accepted Principles and Practices. Set of principles developed by the U. S. National Institute of Standards and Technology (NIST)
- GASSP: Generally Accepted System Security Principles. Set of principles produced by the International Information Security Foundation (I^2SF)
- SSAG: System Self-Assessment Guide for Information Technology Systems. Guidance developed by the U. S. National Institute of Standards and Technology (NIST)

The capability maturity community is based on the notion of the maturity model. This community has only one member:

- SSE-CMM: Systems Security Engineering Capability Maturity Model. Model developed by the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU)

Other models include the security based proprietary models, checklists, and attack taxonomies. Amoroso (1994) defines attack taxonomy as any generalized categorization of potential attacks that might occur on a given computer system. This community has the following members:

- CIA model: Computer Security based on Confidentiality, Integrity, and Availability.
- Proprietary Models
    - ESA: Enterprise Security Architecture developed by PricewaterhouseCoopers
    - ISF: Information Security Framework developed by Arthur Anderson
- Checklists
    - CIAO Practices: Practices for Securing Critical Information Assets developed by the Critical Infrastructure Assurance Office
    - Garfinkel & Spafford Checklist: UNIX and Internet security checklist
    - Levine Checklist: Generic paper on auditing computer security
    - Vallabhaneni Checklist: Security taxonomy based on directive, preventive, detective, corrective and recovery actions
    - GAO Audit Guide: Audit guide developed by the U. S. General Accounting Office
    - Wood's Comprehensive Controls Checklist: Comprehensive Security Controls Checklist developed for the Los Alamos National Laboratories
    - Krauss Guide: Audit and field evaluation guide related to security
    - system specific checklists

- Principles
    - OECD Principle: Set of information security principles developed by the Organization for Economic Cooperation and Development (OECD)
    - NIST's Engineering Principles for IT Security: Security principles developed by the National Institute of Standards and Technology (NIST)
    - IFAC Principle: Principles for managing security of information developed by the International Federation of Accountants
    - Wood's Principles of Secure Information Systems Design
    - GAO's Learning from Leading Organizations: Executive Guide for Information Security Management developed by the U. S. General Accounting Office (GAO)
    - Gaston Security Principles: Security principles
    - Meadows' Taxonomy: Taxonomy of Computer Security Research and Development
- SAC: Systems Auditability and Control. Guideline developed by the Institute of Internal Auditors Research Foundation
- Risk assessment methods
    - Control Self-Assessment (CSA): Risk assessment tool
    - OCTAVE: The Operationally Critical Threat, Asset, and Vulnerability Evaluation. Risk assessment approach developed by Alberts & Dorofee (2002)
- Common Criteria: IT security measures developed by seven countries

- Attack taxonomies: Perry & Wallich (1984), Neumann & Parker (1989), Bernstein et al. (1996), Lindqvist & Johnsson (1997), Benjamin, Gladman & Randell (1998), Howard & Longstaff (1998), Schneider et al. (1999) proposed attack taxonomies on information security, Internet security and network security.
- Miscellaneous models
    - SAS55
    - SAS78
    - Cadbury
    - Orange Book
    - KonTraG
    - UNEDO and UN Guidelines
    - ITIL IT Management Practices: IT Infrastructure Library
    - IBAG Framework
    - PCIE Model Framework
    - IFAC International Information Technology Guidelines
    - Denmark Generally Accepted IT Management Practices
    - C & L Audit Guide SAP R/3
    - ISO IEC JTC1/SC27 Information Technology
    - TickIT
    - ESP Baseline Control
    - PRINCE2

- Marion: French methodology for an in-depth analysis of operational IT risks and IT security

On the other hand, ICMs are classified by Liu & Ridley (2006) into two distinct classes by referring to Bae, Epps & Gwathmey (2003): the business focused control frameworks and the more IT focused control frameworks. Business focused control frameworks include COSO, SAS55, and SAS78. IT focused control frameworks include ITIL, and ISO27001. As it has become necessary for IT to become an integral part of business (Lainhart, 2000), a third class of control frameworks, which align control over IT with business objectives, is desirable. CobiT is the framework that focuses on the alignment of IT control and the achievement of business goals (Bae, Epps & Gwathmey, 2003 & Colbert & Bowen, 1996). Finally, Putnam (2004) also classifies over eighty ICMs under various sub-categories including their sources.

Information Control Models in the Aggregated Checklist

While these are not turn-key methodologies that will embed IT Governance into the organization, the frameworks provide a foundation for creating a structured, risk based and well accepted governance structure. Therefore, the organizations are arguing for the necessity to harmonize and integrate the leading frameworks to achieve greater compatibility. The ICMs covered in this study are listed in Table 7, including their sponsoring organizations and the number of the control objectives in these ICMs. The control objective numbers represent the numbers of the most detailed control objectives in the ICMs.

Table 7: Information Control Models

	Information Control Model	Sponsoring Organizations	Control Objective
1	CobiT	Information Systems Audit and Control Association (ISACA) Information Technology Governance Institute (ITGI)	215
2	BS7799	British Standards Institute (BSI) International Electrotechnical Commission (IEC) United Kingdom Government's Department of Trade and Industry (DTI)	127
3	ISO27001	International Electrotechnical Commission (IEC) International Organization for Standardization (ISO)	133
4	ITIL	Information Technology Service Management Forum (itSMF) United Kingdom's Office of Governance Commerce (OGC)	140
5	COSO	Committee of Sponsoring Organizations of the Treadway Commission (COSO)	39

CobiT (ITGI, 2005) is based on the notion of control adapted from COSO and the control objective adapted from SAC where control objective is a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity (ITGI, 2000). CobiT has 215 control objectives under four domains and thirty-four sub-domains. The CobiT framework is represented in Figure 15. Domains in CobiT are as follows:

- Plan & Organize (PO)
- Acquire & Implement (AI)
- Deliver & Support (DS)
- Monitor & Evaluate (ME)

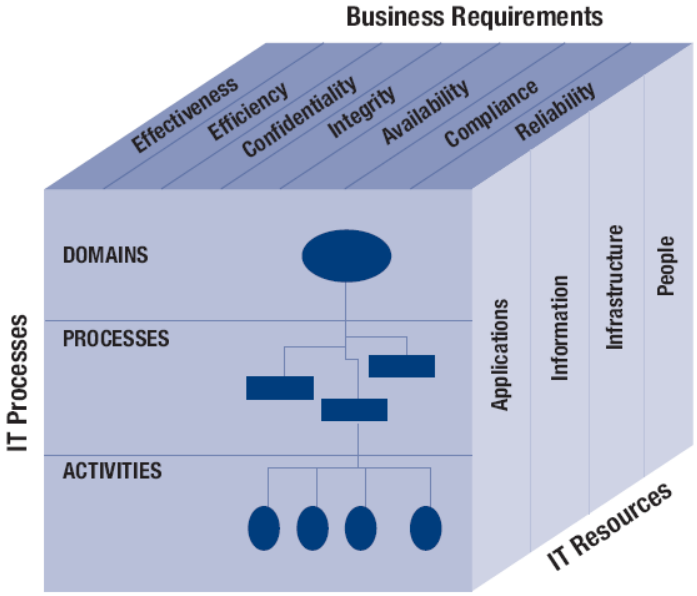

Figure 15: CobiT framework

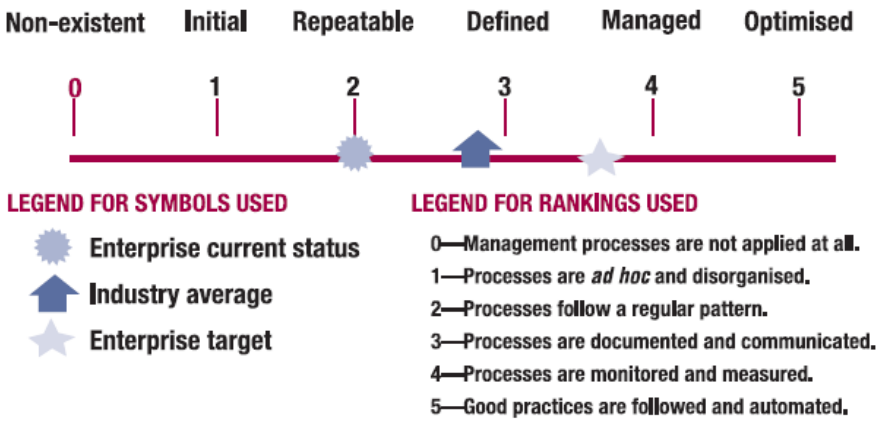

Figure 16: CobiT's maturity model

CobiT also requires the process owner to be able to incrementally benchmark against the control objective and rate in a maturity model. This responds to three needs: (1) A relative measure of where the enterprise is, (2) a manner to efficiently decide where to go, and (3) a tool for measuring progress against the goal. Maturity modelling for

management and control over IT processes is based on a method of evaluating the organization, so it can evaluate itself from a level of non-existent (0) to optimized (5) as in Figure 16.

BS7799 (BSI, 1999) focuses on information security, which is constituted on "BS7799-1:1999 Information security management - Part 1: Code of practice for information security management" and "BS7799-2:1999 Information security management - Part 2: Specification for information security management systems". BS7799 has 127 control objectives under ten domains. Domains in BS7799 are as follows:

- Security policy
- Security organization
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

ISO27001 (ISO, 2005) focuses on information security and is based on BS7799. ISO27001 has 133 control objectives under eleven domains. Domains in ISO27001 are as follows:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

ITIL (OGC, 2004) focuses on the best practice implementation for service management in an organization under fifteen domains. The ITIL framework is shown in Figure 17. ITIL has 140 control objectives under the following domains:

- Business Perspective
- Planning to Implement Service Management
- ICT Infrastructure Management
- Application Management
- Service Delivery: Service Level Management
- Service Delivery: Financial Management for IT Services
- Service Delivery: Capacity Management
- Service Delivery: IT Service Continuity Management

- Service Delivery: Availability Management
- Service Support: The Service Desk
- Service Support: Incident Management
- Service Support: Problem Management
- Service Support: Configuration Management
- Service Support: Change Management
- Service Support: Release Management

Figure 17: ITIL framework

COSO (COSO, 2004) emphasizes the responsibilities of management for control, and the key principles for creating an effective risk management process, in order to help businesses and other entities to assess and enhance their internal control systems in the enterprise risk management (ERM) framework shown in Figure 18. The COSO ERM framework has thirty-nine control objectives under eight components. Each control

objective has questions as a checklist in order to ensure that management is aware of the control framework. Components in the COSO ERM framework are as follows:

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

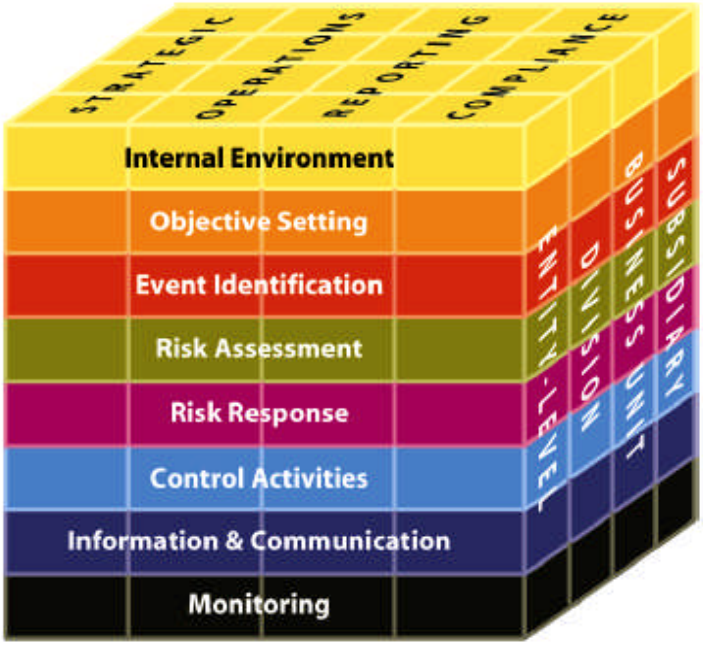

Figure 18: COSO ERM framework

COSO had an internal control framework before the ERM framework, which is still in use. The internal control framework is designed under five components: control environment, risk assessment, control activities, information and communication, and monitoring (COSO, 1992). Although many ICMs refer to the internal control framework, the ERM framework has been considered in the thesis in order to be able to assess the risk management approach of COSO rather than its internal control structure.

Ames (2005) tabulates the COSO, ITIL, and CobiT control structures as in Tables 8, 9, and 10. The structure is based on strategic analysis and future actions, based on the value of the business process, risks in the process, actions to be taken in order to prevent risks, experience gained in order to prevent risks, future risks, and a prediction about the risk.

Table 8: COSO Control Structure

	Strategic Analysis	Future Action
Value	Clearly identify business objectives	Translate objectives into policy
Risks	Management policies and decisions are not carried through	Establish effective implementation and monitoring
Actions	Identify threats, opportunities, control weaknesses	Develop an effective control structure
Experience	Poorly articulated objectives and weak control structures lead to financial losses	Monitor objectives effectiveness of control structures
Future	Control structures deteriorate without maintenance	Review and enhance control structures regularly
Prediction	Business success improves with effective risk management and internal control	All of the above!

Table 9: ITIL Control Structure

	Strategic Analysis	Future Action
Value	Business processes require specific services and service levels	Define service levels
Risks	Services may not be performed as required	Establish effective metrics and monitoring
Actions	Threats to service delivery could impact the objectives	Identify and address performance problems
Experience	Poorly defined objectives and deficient	Review objectives and improve processes

	processes impact business performance	regularly
Future	Ongoing improvement is required to maintain performance	Commit the continuous improvement
Prediction	Business success improves the effective service delivery	All of the above!

Table 10: CobiT Control Structure

	Strategic Analysis	Future Action
Value	Decrease probability of adverse consequences and limit impact on the business	Identify control objectives, document control statements
Risks	Control objectives may not be met	Define and monitor control practices
Actions	Monitor effectiveness of control practices	Monitor effectiveness of control practices
Experience	Poorly defined control objectives and deficient processes impact business performance	Review control objectives and improve processes regularly
Future	Control practices deteriorate without maintenance	Commit the continuous improvement
Prediction	Business success improves with effective management of IT controls	All of the above!

Finally, a new control structure for BS7799 and ISO27001 is designed together since they focus on security issues, considering the concept in Ames's (2005) control structures shown in Table 11.

Table 11: BS7799 and ISO27001 Control Structure

	Strategic Analysis	Future Action
Value	Decrease probability of adverse consequences and limit impact on the business by defining the security requirements	Identify control objectives, document control statements
Risks	Security incidents may affect the business	Define and monitor control practices
Actions	Monitor effectiveness of control practices	Monitor effectiveness of control practices
Experience	Poorly defined control objectives and deficient processes impact business performance	Review control objectives and improve processes regularly
Future	Control practices deteriorate without maintenance	Commit the continuous improvement
Prediction	Business success improves with effective management of IT security controls	All of the above!

CHAPTER THREE

LITERATURE REVIEW

In order to manage operational risk, different tools, techniques and standards have been proposed referring to ICMs that we have discussed in the previous chapters and to Basel II. Some of the proposed ORM models are summarized in order to formalize and assess propositions and recommendations responding to operational risks within the context of financial and banking industry.

A Practical Framework for Operational Risk Management

Loewenton (2003) proposed a practical framework for operational risk management that would include the following topics:

- Risk Identification & Assessment: This is usually done through a risk and control self-assessment (RCSA) program.
- Risk Quantification & Measurement: A quantitative method using the internal loss data is applied to calculate the risk exposure.
- Risk Analysis, Monitor & Reporting: Analysis of risk, monitoring of risk exposure, and action plans should be appropriate for various levels of ORM.
- Risk Capital Allocation: Operational regulatory capital is calculated for every business line to protect from unexpected.
- Risk Management & Mitigation: Actions that plan a risk free environment

Loewenton (2003) also suggests implementing knowledge management systems within such a framework in order to manage the risk management process. Thus, banks are able to document, to archive and to codify explicit and tacit knowledge (know-how and expertise contained in people's heads). This will reduce the loss of technical knowledge and expertise and will also increase the chance of mitigating operational risks as the best knowledge will be available at every place and time. Such a platform can be used to handle the documentation of the different workflow, methods and procedures, to allow easy access to special handling processes in case of a system failure or incident (which often causes a great deal of manual activities that people tend to forget as they seldom execute them), and to manage the business continuity plan and all other types of information disseminated in the company. Another benefit of such a system in an operational risk management project is the possibility of using all the information about loss events whilst all figures and data useful for the quantification and measurement of operational risk can be logged or fed automatically into a database.

Mission Assurance Analysis Protocol (MAAP)

Because conventional techniques proved to be inadequate for analyzing operational risk in complex processes, Alberts & Dorofee (2005) have proposed a new approach. Their development effort produced MAAP, which is specifically designed to analyze operational risk in distributed work processes. Although MAAP was specifically designed with distributed processes in mind, it can also be used to analyze the effects of operational risk on simpler workflows.

MAAP defines a protocol for analyzing operational risk in work processes. Alberts & Dorofee (2005) summarize the basic and fundamental principles underlying the protocol. The following seven guidelines collectively form the foundation of MAAP:

1. Determine mission objectives.
2. Characterize all operations conducted in pursuit of the mission.
3. Define risk evaluation criteria in relation to the mission objectives.
4. Identify potential failure modes.
5. Perform a root cause analysis for each failure mode.
6. Develop an operational risk profile of the mission.
7. Ensure that operational risk is within tolerance.

Rather than designing MAAP to analyze risk in a specific type of work process, such as a software development process or an operational security process, Alberts & Dorofee (2005) chose to develop a general risk analysis approach that is applicable across a wide variety of processes. In this way, one risk analysis technique could be applied to numerous operational settings, obviating the need for multiple specialized assessment techniques. The General Risk Analysis Approach illustrates the notion that MAAP provides a foundation for analyzing risk in a variety of domains as shown in Figure 19.

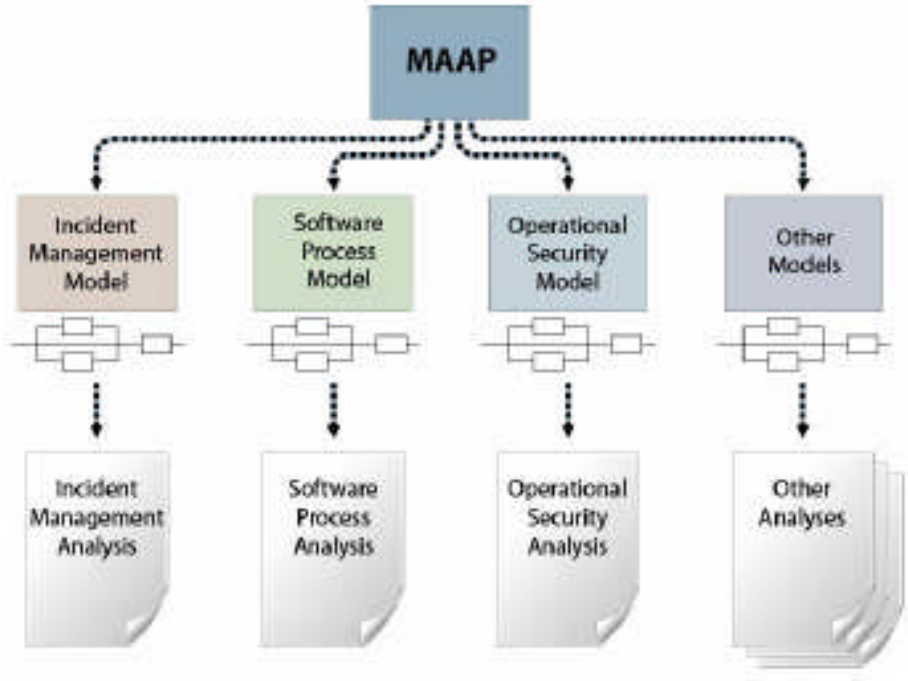

Figure 19: General risk analysis approach

Operational Risk Management Maturity Model (ORMMM)

Mc Connell (2005) proposed a starting point to develop an Operational Risk Management Maturity Model (ORMMM) by discussing and combining the COSO and Capacity Maturity Model Integration (CMMI) (SEI, 2002) in order to measure the operational risks using a capability maturity model based on the risk management framework. In order to integrate the concept of risk management and the capability maturity model, each key principle in COSO would have to be re-phrased in such a way that (instead of a simple Yes/No answer) compliance with a particular principle could be evaluated on a five point scale. The proposed ORMMM levels are presented in Table 12.

Table 12: Proposed Operational Risk Management Maturity Model

Maturity Level	Criteria	Relevance of COSO
1 Initial	Management recognizes that ORM needs to be addressed but there are no standardized processes in place and operational risk issues (such as major losses) are only addressed reactively.	There is no awareness of the COSO framework or other comprehensive risk management models.
2 Managed	Management is aware of ORM issues, and selected processes have been identified and implemented, but standardized measurement has not been implemented across the organization.	Selected components of the COSO have been implemented across selected businesses (e.g. consistent Risk Assessment). ORM organizational structures have been identified but not fully staffed. Management reacts to crises.
3 Defined	Standardized ORM processes are in place across the organization, performance is being monitored but root cause analysis of problems is only occasionally being applied.	The COSO has been implemented across those businesses with the most operational risk. ORM staffing is complete. No consistent quantitative measurements of performance are in place and management actions are initiated only to address critical issues.
4 Quantitatively Managed	Standardized processes are in place and responsibilities and process ownerships are clearly defined. ORM processes are aligned with the business strategy. Quantitative measurements, such as Key Risk Indicators (KRI), are in place for all processes and economic capital is being allocated against these measures. However, there are no continuous improvement programs in place to align operational risk with the organization's risk appetite.	All components of the COSO have been implemented across most businesses. Consistent monitoring is in place and information flows to all levels of management. External experts are employed to assess the operation of all processes. Management actions are initiated to reduce areas of significant operational risk.
5 Optimized	Best practice ORM processes are in place and are closely aligned with business strategies. Costs and benefits of operational risk management are defined, are balanced against risks and are communicated and applied across the whole organization.	The full COSO framework is in place across the organization and being applied by all levels of management. Management has funded plans to improve the level of ORM maturity of all businesses.

Mc Connell (2005) refers to Lainhart (2001) where he identifies some of the benefits of taking a maturity model approach to process implementation and improvement in IT, which can be generalized to other complex management processes. He notes that a maturity model, such as CMMI:

- Provides a scale that lends itself to pragmatic comparison between implementations of the same process in different situations.

- Provides a scale where differences can be easily measured.
- Is recognizable as a profile of the enterprise in relation to a particular process.
- Assists in determining As-Is, Should-Be and To-Be positions relative to a process and its maturity.
- Lends itself to doing Gap Analysis to determine what needs To-Be done to achieve a chosen maturity level for a particular process.
- Is not industry specific or generally applicable since the nature of the business will determine what the appropriate level is.

Mc Connell (2005) suggested that the numeric score for all key principles could then be averaged (with some weighting of individual categories if necessary) to produce an overall score for the ORM maturity of the business/organization being evaluated. A colored heat map that summarizes the current state of ORM systems across an organization, using the classification of business lines mandated by Basel II against the high-level components of COSO is proposed to provide practical tools to assist executive boards and management, in developing and improving their ORM.

CHAPTER FOUR

METHODOLOGY

Basel II Requirement Analysis

The improvement of banks' operational risk management frameworks concerns new requirements addressed in Basel II (Di Renzo & Bernard, 2005). The main sources are the publications of the Basel Committee: Basel II (Basel Committee, 2004), and a document entitled Sound Practices for the Management and Supervision of Operational Risk (Basel Committee, 2003a). Other important sources were the workshops organized and the documents published by the Basel Committee (2001a, 2001b, 2001c, 2001d, 2002a, 2002b, 2002c, 2003a, 2003b, 2004) where supervisors described their expectations form banks' ORM framework and the assessments' organizational constraints. Then, the descriptions of ICMs and ORM methods and good practices, including loss data analyses, were used. Finally, the articles and case studies structured on the operational failures of the companies were read and interpreted.

As mentioned, three approaches are proposed in Basel II for the calculation of minimum capital requirements for operational risk. So, the requirements were structured along those three approaches. For instance, the requirement that as part of the bank's internal risk assessment system, the bank must systematically track relevant operational risk data including material losses by business lines (Basel Committee, 2004, p.663) is essential to the SA. Moreover, these approaches are ranked in increasing order of sophistication. The more advanced approach encompasses the requirements of the less

sophisticated approaches. This structure has been adopted for the definition of the categories of requirements. For instance, if a bank adopts an AMA, it will have to meet the following requirement: Any internal risk measurement system must be consistent with … the loss event types … (Basel Committee, 2004, p.669) in addition to the requirement given above for the SA.

The structure of risk management activities can also be gathered from the requirements. For instance, the requirement that the ORM function must be responsible for developing strategies to identify, assess, monitor, and control/mitigate operational risk (Basel Committee, 2004, p.663), indicates activities composing the management of risks. In this example, the following activities are identified: Risk identification, Risk assessment, Risk monitoring and Risk mitigation/control.

Some requirements refer to a clear assignment of responsibilities and authorities, such as the requirement that the bank must have techniques for creating incentives to improve the management of operational risk throughout the firm (Basel Committee, 2004, p.663). This example shows that financial and managerial incentives must be used in order to ensure that each bank employee contributes to the improvement of the operational risk management framework.

Since Basel II requires a supervisory review process including the assessment of the control environment, it is also required that supervisors should consider the quality of the bank's management information reporting and systems, the manner in which business risks and activities are aggregated, and management's record in responding to emerging or changing risks (Basel Committee, 2004, p.751). In addition, Basel II requires that the bank have clear and effective policies, procedures, and information systems to monitor compliance with … (Basel Committee, 2004, p.496), that each

supervisor develop detailed review procedures to ensure that banks' systems and controls are adequate to serve … (Basel Committee, 2004, p.6 & p.389), and that management must also ensure, on an ongoing basis, that the rating system is operating properly (Basel Committee, 2004, p.439) in different sections.

In addition to Basel II itself, ITGI (2007b) published a draft document entitled IT Control Objectives for Basel II on 9 May 2007. ITGI (2007b) is taking the proactive step of addressing risk in financial service organizations, regarding that information risk and information technology have become decisive factors in shaping modern business, and many financial service organizations have undergone a fundamental transformation in terms of IT infrastructures, applications, and IT related internal controls. Since IT related components such as applications, infrastructure elements and controls are all defined as parts of operational risk, ITGI (2007b) maps Basel II principles for operational risk against information technology risk.

Therefore, ITGI (2007b) defines a set of ten guiding principles for information risk management, where these guiding principles correspond to the principles of ORM as set down in Basel II, and where these risks are related to IT scenarios and controls. The ten IT guiding principles (ITGP) developed by ITGI (2007b) are as follows:

1. ITGP1: Operational Risk Awareness
2. ITGP2: Internal Audit Requirement
3. ITGP3: Management Policies, Processes, Procedures
4. ITGP4: Risk Assessment
5. ITGP5: Risk and Loss Monitoring
6. ITGP6: Control and Mitigation Policies, Processes, Procedures
7. ITGP7: Business Continuity Management

8. ITGP8: Framework for Risk Control and Mitigation
9. ITGP9: Independent Evaluation
10. ITGP10: Disclosure

These ten principles are established on the ten Basel II principles and their IT relevance and requirements by ITGI (2007b). Thus, the requirements in Basel II and their impacts on IT are evaluated and a RGC framework based on ITGPs is established. The core Basel II principles are listed as follows:

1. Board of directors should be aware of the need for an operational risk management framework.
2. Operational risk management framework is subject to effective and comprehensive internal audit.
3. Develop policies, processes and procedures for managing operational risk.
4. Identify and assess the operational risk.
5. Regularly monitor operational risk profiles and material exposures to losses.
6. Have policies, processes and procedures to control and/or mitigate material operational risks.
7. Have contingency and business continuity plans.
8. Have framework in place to identify, assess, monitor and control/ mitigate material operational risks.
9. Conduct regular independent evaluation of a bank's policies, procedures and practices related to operational risks.
10. Sufficient public disclosure.

ITGI (2007b) refers only to the CobiT framework at sub-domain level by bridging the Basel II principles and CobiT principles, rather than to the control objective level. In addition, ITGI (2007b) builds an ORM framework, which sets the principles and guides the stakeholders rather than proposing a new ICM for ORM. However, ITGI (2007b) brings the concepts of risk management, corporate and IT Governance, ICMs, and related regulations, and highlights the importance of corporate governance, risk management, and regulatory compliance (GRC). Therefore, the aim of this paper has been to assess whether IT Governance frameworks and standards (information control models) are appropriate at the control objective level for controlling the operational risks, and to integrate and harmonize them in order to project an aggregated IT checklist for ORM. In the following sections, the methodology used while establishing the aggregated IT checklist for ORM is detailed.

Mapping Information Control Models to Operational Risks

Each and every control objective in ICMs, which are covered in this study, have been mapped to the seven loss event types defined in Basel II (Basel Committee, 2004, annex.7), which are also operational risk categories (Basel Committee, 2004, p.669). In the same way, each and every control objective in ICMs have been mapped to the three control types defined by ITGI (2005): preventive, detective, and corrective. In order to be able to scale the contribution level of each ICM and the penetration level of each control objective smoothly, one-to-one mapping has been performed. However, one-to-one mapping caused an underestimation of the secondary mapping alternatives since

control objectives may have an impact on other operational risk categories and additionally on different control types.

While mapping the control objectives, their nature is considered. For example, a control objective may be attained by applying preventive, detective or corrective control at different levels and steps of a process. However, the goal of the control objective is used as the motivation on which the mapping is based, e.g. if the control objective is about monitoring a process, it is mapped to a detective control. In the same way, a control objective may cover the internal fraud or external fraud risk. However, the prior objective of the control objective is used as the motivation on which the mapping is based, e.g. if the control objective is about access rights, it is mapped to internal fraud, rather than considering the access rights of the third parties, since there are different objectives related to relationships with third parties.

Therefore, the loss event type activities exampled in Basel II have been extended in order to cover the context, domains, controls and IT based activities in ICMs so that a guideline for mapping is prepared. For loss event types, the following activities have been added:

- Internal Fraud: Roles and responsibilities, segregation of duties, data ownership, user account and identity management, promotion to production, logging mechanism.
- External Fraud: Contracted staff security, external network security, external network connections, exchange of data.
- Employment Practices and Workplace Safety: Organizational structure, staffing, competencies, staff evaluation, training.

- Clients, Products & Business Practices: Policies, procedures and standards, control environment, IT strategy and business practices alignment, IT risk management, IT supervisory and advisory boards, IT budgeting, enterprise IT models (business / technical requirements), portfolio management, value management and delivery, resource management, database management, data classification, data confidentiality.
- Damage to Physical Assets: Site selection and layout, external facilities, offsite storage, media library management, access to physical assets and sensitive documents, disposal.
- Business Disruption and System Failures: Disaster Recovery Plan, Business Continuity Plan, configuration, infrastructure, incident, problem and change management, service desk, development activities, release and distribution, update and upgrade, testing, back-up and recovery.
- Execution, Delivery & Process Management: Service Level Agreements, performance monitoring, key personnel, scheduling, reporting, data integrity, data processing.

Focus Group Assessment

While mapping the control objectives to the operational risk categories, we organized a workshop in order to ensure the reliability of the study. External IT auditors from consultancy services, internal auditors from the business world, and professionals from academic institutions participated in the workshop and served as judges by assessing the

proposed mappings between the control objectives in CobiT, operational risk categories and control types. Since other ICMs have been mapped to CobiT (ITGI, 2006a and ITGI, 2007a), the focus group assessed only the CobiT and Basel II mapping that I proposed before the workshop, in the workshop. Thus, the focus group increased the validity and reliability of the study since the mappings are based on subjective appraisals.

In order to be able to assess the mappings, the focus group was informed about the operational risk categories, the loss event type examples based on IT, and the control types with an invitation letter. The letter included the basic concepts related to the ORM and ICMs before the workshop and with a presentation during the workshop. Thus, the focus group had a common understanding of the concepts covered in the aggregated IT checklist.

During the workshop, the focus group discussed each control objective in CobiT and accepted the mapping or rejected it and proposed a new mapping. The control objectives were ordered according to the operational risk categories proposed, and discussed in this order. Therefore, the participants had a wider view of the context of each operational risk category and a chance to comprehend and compare the control objectives in a specific operational risk category. Additionally, the participants were requested to write down their choice of mappings on the set of documents as evidence. The participants are listed in Appendix A.

Table 13 shows us the results of the deviation analysis between the proposed mapping and the mapping performed during the workshop regarding the control objectives in CobiT. The detailed mappings are given in Appendix B. The number of control objectives in the mapping category represents the numbers that the focus group

decided on. The number of complied mapping regarding loss event type, control type, and both represent the numbers of the control objectives for which the focus group has affirmed the proposed mapping. The results show us that the proposed mappings were relevant for 188 control objectives out of 215 control objectives regarding only loss event type, for 182 control objectives out of 215 control objectives regarding only control type, and for 156 control objectives out of 215 control objectives regarding both, that is with 87.44%, 84.65%, and 72.56% confidence levels respectively.

Table 13: Deviation Analysis between Proposed Mapping and Workshop Results

Mapping Category		Number of Control Objectives in the Mapping Category	Number of Complied Mapping (Loss Event Type and Control Type)	Number of Complied Mapping (Loss Event Type)	Number of Complied Mapping (Control Type)
Internal Fraud	Detective	1	1	1	1
	Preventive	11	7	7	11
External Fraud	Detective	1	1	1	1
	Preventive	4	3	3	4
Employment Practices and Workplace Safety	Corrective	2	1	2	1
	Detective	3	3	3	3
	Preventive	12	11	12	11
Clients, Products & Business Practices	Corrective	3	3	3	3
	Detective	7	5	6	6
	Preventive	55	40	43	51
Damage to Physical Assets	Preventive	11	10	11	10
Business Disruption and System Failures	Corrective	3	2	3	2
	Detective	5	3	5	3
	Preventive	24	14	21	17
Execution, Delivery & Process Management	Corrective	9	9	9	9
	Detective	28	22	26	24
	Preventive	36	21	32	25
Grand Total		215	156	188	182

Table 14 summarizes the differences between the proposed mappings and the focus group assessment results in each operational risk category and control type where applicable.

Table 14: Differences between Proposed Mappings and Workshop Results

Mapping Category		Focus Group Assessment Results	Number of Proposed Mapping
Internal Fraud	Detective	1	3
	Preventive	11	10
External Fraud	Detective	1	1
	Preventive	4	3
Employment Practices and Workplace Safety	Corrective	2	1
	Detective	3	5
	Preventive	12	14
Clients, Products & Business Practices	Corrective	3	6
	Detective	7	6
	Preventive	55	46
Damage to Physical Assets	Detective	0	1
	Preventive	11	10
Business Disruption and System Failures	Corrective	3	8
	Detective	5	6
	Preventive	24	24
Execution, Delivery & Process Management	Corrective	9	15
	Detective	28	31
	Preventive	36	25
Grand Total		215	215

Table 15 presents the consensus within the focus group while mapping the control objectives in CobiT with the decision of the majority or unanimous agreement. The detailed consensus results are given in Appendix B. The results show us that the focus group generally reached a consensus, especially for the security related issues such as internal fraud, external fraud and damage to physical assets. Since there was a discussion on the IT activities regarding business continuity, whether it should be categorized under business disruption and system failures or execution, delivery & process management, the consensus on these areas are lower than the others. There are seventeen control

objectives where the focus group made a majority decision, and 198 control objectives where the focus group was unanimous in its decision while mapping the control objectives in CobiT.

Table 15: Workshop Consensus Results

Operational Risk Category	Workshop Results	Number of Control Objective
Internal Fraud	Decision with majority	1
	Decision with unanimity	11
External Fraud	Decision with majority	1
	Decision with unanimity	4
Employment Practices and Workplace Safety	Decision with majority	2
	Decision with unanimity	15
Clients, Products & Business Practices	Decision with majority	2
	Decision with unanimity	63
Damage to Physical Assets	Decision with unanimity	11
Business Disruption and System Failures	Decision with majority	4
	Decision with unanimity	28
Execution, Delivery & Process Management	Decision with majority	7
	Decision with unanimity	66
Grand Total		215

Gap Analysis

Using the mapping results for CobiT's control objectives, performed during the workshop and mappings between CobiT and other ICMs (ITGI, 2006a and ITGI, 2007a), control objectives in BS7799, ISO27001, ITIL and COSO have been mapped to the operational risk categories and control types. As a result, a gap analysis between ICMs is done by calculating the contribution and penetration levels of each ICM in each operational risk category and control type.

The contribution level is the percentage of the control objectives in an ICM dedicated to a specific operational risk category in Basel II, considering all control

objectives in that ICM. The contribution level indicates how many control objectives in an ICM are covering which operational risk category in Basel II. The penetration level is the percentage of the control objectives in an ICM, dedicated to a specific operational risk category in Basel II and to a specific control type, considering all control objectives in that ICM. The penetration level indicates how many control objectives in an ICM are covering which operational risk category in Basel II and in which nature. It is possible to understand which ICM focuses on which operational risk category by interpreting the contribution level. It is possible to understand which ICM focuses on which operational risk category and in which nature of control by interpreting the penetration level.

After mapping the control objectives in ICMs to the operational risk categories and control types, the contribution level of each ICM for each operational risk category has been calculated using the following formula:

$CL_{ICM} = CO_{R} / COT_{ICM} * 100$ as

CL_{ICM}: Contribution Level of ICM for the Operational Risk Category
CO_{R}: Number of Control Objectives in ICM mapped to the Operational Risk Category
COT_{ICM}: Total Number of Control Objectives in ICM.

In the same way, the penetration level of each ICM for each operational risk category and each control type has been calculated using the following formula:

$PL_{ICM} = CO_{RT} / COT_{ICM} * 100$ as

PL_{ICM}: Penetration Level of ICM for the Operational Risk Category and Control Type

CO_{RT}: Number of Control Objectives in ICM mapped to the Operational Risk Category and Control Type

COT_{ICM}: Total Number of Control Objectives in ICM.

CHAPTER FIVE

FINDINGS

Contribution and Penetration Levels of Information Control Models

The contribution and penetration levels of each ICM are presented in Table 16. These levels show us the characteristics of the control objectives in ICMs considering the operational risk categories and control types.

The table points out that the ICMs have mostly preventive control objectives rather than detective and corrective control objectives, e.g. there are no corrective controls for external fraud or damage to physical assets risk categories.

The table shows us that CobiT is the best practice regarding the Employment Practices and Workplace Safety, Clients, Products & Business Practices, and Execution, Delivery & Process Management operational risk categories if we consider that COSO is a risk management framework rather than an IT Governance standard. ISO27001 is the best practice regarding the Internal Fraud and Damage to Physical Assets operational risk categories. BS7799 is the best practice regarding External Fraud, and ITIL is the best practice regarding the Business Disruption and System Failures operational risk category.

As a result, the results are in line with the nature of ICM since BS7799 and ISO27001 focus on security and ITIL focuses on change management, availability management, and problem management.

Table 16: Contribution and Penetration Levels of Information Control Models

(in percentage)

Operational Risks	Impact	Control Type	CobiT	BS7799	ISO27001	ITIL	COSO
Internal Fraud	CL	Total	5.58	25.20	26.32	2.14	2.56
	PL	Preventive	5.12	22.05	23.31	2.14	2.56
		Detective	0.47	2.36	2.26	0.00	0.00
		Corrective	0.00	0.79	0.75	0.00	0.00
External Fraud	CL	Total	2.33	18.11	16.54	0.00	0.00
	PL	Preventive	1.86	15.75	13.53	0.00	0.00
		Detective	0.47	2.36	3.01	0.00	0.00
		Corrective	0.00	0.00	0.00	0.00	0.00
Employment Practices and Workplace Safety	CL	Total	7.91	3.15	3.01	2.14	10.26
	PL	Preventive	5.58	2.36	2.26	2.14	10.26
		Detective	1.40	0.00	0.00	0.00	0.00
		Corrective	0.93	0.79	0.75	0.00	0.00
Clients, Products & Business Practices	CL	Total	30.23	13.39	12.78	26.43	56.41
	PL	Preventive	25.58	11.02	10.53	20.00	56.41
		Detective	3.26	2.36	2.26	6.43	0.00
		Corrective	1.40	0.00	0.00	0.00	0.00
Damage to Physical Assets	CL	Total	5.12	15.75	15.79	0.71	0.00
	PL	Preventive	5.12	14.96	15.04	0.71	0.00
		Detective	0.00	0.79	0.75	0.00	0.00
		Corrective	0.00	0.00	0.00	0.00	0.00
Business Disruption and System Failures	CL	Total	14.88	15.75	15.79	41.43	15.38
	PL	Preventive	11.16	9.45	9.77	25.71	5.13
		Detective	2.33	4.72	5.26	12.86	10.26
		Corrective	1.40	1.57	0.75	2.86	0.00
Execution, Delivery & Process Management	CL	Total	33.95	8.66	9.77	27.14	15.38
	PL	Preventive	16.74	4.72	4.51	12.14	0.00
		Detective	13.02	3.94	5.26	10.71	15.38
		Corrective	4.19	0.00	0.00	4.29	0.00

As shown in Table 16, COSO concentrated on the business practices, process management and business disruption. BS7799 and ISO27001 have similar contribution and penetration levels since they are security standards, and ISO27001 has been developed using BS7799. Therefore, they have higher contribution and penetration levels especially for internal and external frauds, and damage to physical assets. In addition, CobiT focuses on the employment practices, business practices and process management, as it is an IT Governance framework and has control objectives designed for support and delivery of IT services. ITIL concentrates on the business disruptions

since it has specific domains related to incident, problem, availability and change management.

Best Practices Approach based on CobiT

The gap analysis between the ICMs and the workshop results leads us to recommend an aggregated IT checklist for ORM since the ICMs covered in this study contribute to the operational risk categories at different levels and penetrate into them in different natures considering the control types. Although the importance of IT controls is embedded in the COSO internal control framework, IT management requires more examples to help identify, document and evaluate IT controls (ITGI, 2004). In addition, PCAOB, the regulatory body established by US legislators to oversee companies' (and auditors') compliance with the Sarbanes-Oxley, recommends the COSO framework as a minimum standard (Datardina, 2005). Therefore, we recommend that COSO to be implemented as a starting point by each organization in order to enable the management of operational risks, because COSO is a risk management framework, and companies are starting to move away from considering their risks in isolation, and are looking beyond the traditional hazard and financial risk towards strategic and operational risks (GIRO, 2002).

The COSO approach refers to ERM, which has been viewed as the management of business risk, financial risk, operational risk and risk transfer to maximize a firm's value to owners and customers (Norris & Young, 2005). Risk transfer is the exchange of the unknown financial impact of specified events to a third party for a known financial

cost through insurance or securitization (Dowd, 2001). Finally, COSO (2004) itself defines ERM as a process, affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

In addition to COSO, the CobiT IT Governance framework is recommended as a baseline since effective IT Governance requires control over IT processes (Payne, 2003) as in CobiT, considering that IT processes cover the setting of objectives, giving directions on how to attain objectives and measuring performance in completing these activities (Korac-Kakabadse & Kakabadse, 2001). To improve the overall performance of IT and reduce the failure caused by inappropriate IT activities, there is a need for careful design, planning, acquisition and implementation of IT to manage its various activities and risks (Beaumaster, 2002 & Hardy, 2002). It is important to properly manage IT resources through a set of IT processes that provide the information which the enterprise needs to achieve its objectives (Payne, 2003). CobiT is based on international best practices from various countries, including the United States of America, Europe, Australia, Canada and Japan; therefore, it serves as a more than appropriate framework on which the comparative framework can be based (Bornman & Labuschagne, 2006). Moreover, CobiT has been regularly accepted and applied by the Turkish banks since 2006 (BRSA, 2006b), and aligns with the spirit of the Sarbanes-Oxley requirement that any framework used be open and generally acceptable (ITGI, 2004). As a result, CobiT bridges the gaps between business risks, control needs, and

technical issues, and we recommend that CobiT to be a baseline although it is not best practice for each operational risk category in Basel II.

Therefore, we recommend additional control objectives of the best practices to be added to CobiT for the operational risk categories in which it is not best practice. In addition, referring to the proposal of CobiT, Hardy (1995) defines CobiT as a common framework, which is cumulative instead of exclusive and based on forty-one primary reference materials. While determining the additional control objectives, control objectives assigned to operational risk categories in CobiT have been mapped to the control objectives in best practice. Thus, only different control objectives have been added and the overlapping of control objectives has been avoided.

Table 17: Aggregated IT Checklist for Operational Risk Management

Operational Risks	Best Practice	Control Objectives in CobiT	Control Objectives in Best Practice	Additional Control Objectives for CobiT
Internal Fraud	ISO27001	12	35	27
External Fraud	BS7799	5	23	15
Employment Practices and Workplace Safety	CobiT	17	17	N/A
Clients, Products & Business Practices	CobiT	65	65	N/A
Damage to Physical Assets	ISO27001	11	21	12
Business Disruption and System Failures	ITIL	32	58	29
Execution, Delivery & Process Management	CobiT	73	73	N/A

Table 17 shows us the structure of the aggregated IT checklist for ORM. Although COSO is best practice considering the Employment Practices and Workplace Safety, and Clients, Products & Business Practices operational risk categories, CobiT is considered as best practice in these areas since COSO is recommended as a starting point of risk management. For Employment Practices and Workplace Safety, Clients, Products & Business Practices and Execution, Delivery & Process Management, the control

objectives of CobiT are appropriate to cover operational risks in these areas. Therefore, there is no need for additional control objectives. For Internal Fraud, twenty-seven additional control objectives from ISO27001 are required in order to able to cover operational risks in this area. In the same way, for External Fraud, fifteen additional control objectives from BS7799 are required, for Damage to Physical Assets, twelve additional control objectives from ISO27001 are required, and for Business Disruption and System Failures, twenty-nine additional control objectives from ITIL are required. The additional control objectives for each ICM are listed in Appendix C.

As a result, COSO and CobiT serve as the starting point of the aggregated IT checklist for ORM since CobiT relates to COSO at a broad level and it is relatively simple to combine COSO with CobiT at a conceptual level (Panko, 2006), as illustrated in Figure 20.

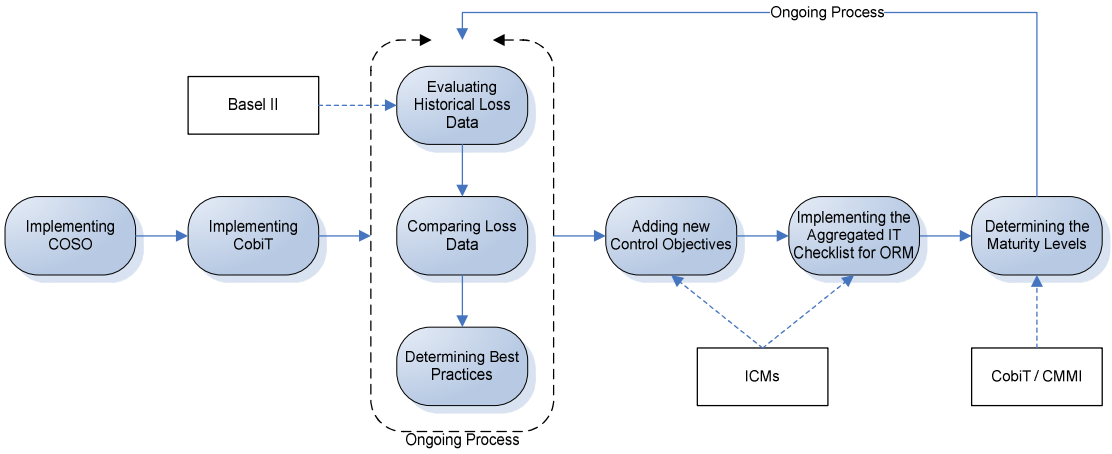

Figure 20: Best practices approach based on CobiT

As shown in Figure 20, the assessment of the operational risks categorized in Basel II is performed using a maturity model, which is derived from CobiT. The control objectives

in the aggregated IT checklist for ORM are assessed using the maturity levels detailed in CobiT (ITGI, 2005) or in CMMI (SEI, 2002) as shown in Table 18.

Table 18: Maturity Levels

Maturity Level	CobiT	CMMI
0	Non-existent	N/A
1	Initial / Ad-hoc	Initial
2	Repeatable but Intuitive	Managed
3	Defined Process	Defined
4	Managed and Measurable	Quantitatively Managed
5	Optimized	Optimized

CHAPTER SIX

CONCULUSION

As explained above, an aggregated IT checklist for ORM is a combined ICM, which is based on COSO and CobiT and expanded using the control objectives from BS7799, ISO27001, and ITIL where they are best practices in specific operational risk category defined in Basel II. Since organizations may have different frequency and severity matrices regarding each operational risk category, they have a chance to apply the aggregated IT checklist as a whole or separately according to the evaluation of their loss data history by comparing the QIS2 results (RMG, 2002) or later researches.

Accordingly, each organization should tailor an IT control approach suitable to its size and complexity, considering the COSO ERM framework (ITGI, 2004), and should develop its GRC (ITGI, 2007b). The aggregated IT checklist for ORM, which is actually a best practices approach based on CobiT, responds to Basel II ORM requirements by comparing the ICMs at the control objective level regarding their penetration and contribution levels to ORM, rather than offering guidance for ORM steps.

The managers and internal or external audit mechanisms can use this study as an operational risk assessment tool by rating each control objective as Mc Connell (2005) discusses such a measurement need. The assessment of the operational risks categorized in Basel II is performed using a maturity model, which is derived from CobiT. The control objectives in the aggregated IT checklist for ORM are assessed using the maturity levels detailed in CobiT (ITGI, 2005) or in CMMI (SEI, 2002).

For further research, a guideline for assessing the maturity levels of the control objectives coming from CobiT and other ICMs can be prepared in order to evaluate the maturity level of each control objective and to assess the ORM in an organization as a whole. In addition, other ICMs might be evaluated according to the operational risk categories in Basel II, considering that different IT processes need the guidance of various models specified in these areas. Since the ICMs discussed in this study are updated according to the business world's requirements, such as new editions of CobiT, where CobiT 4.1 has been published during the documentation of the study, and ITIL, where ITIL 3.0 is going to be published in the third quarter of 2007, the study should be revised and updated accordingly.

With so much to do and so little time or resources, the operational risk managers need to prioritize the steps in ORM and apply the 80/20 rule (Lanz, 2002). By focusing on and assigning resources to high-priority risks and exposures, operational risk managers can cost-effectively mitigate risk to an acceptable level for their enterprise. Independently from the methods and models employed during the ORM process, organizations should not forget Hoffman's (2002) statement: all the risk management in the world cannot compensate for a flawed corporate vision and culture.

REFERENCES

Aktolun, O. (2002). *Bilgi teknolojileri denetim yaklaşımı*. Ankara: Deloitte & Touche, and Turkish Banking Association.

Alberts, C. (2006). *Common elements of risk*. Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Alberts, C. & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach*. Boston: Addison-Wesley.

Alberts, C. & Dorofee, A. (2005). *Mission assurance analysis protocol (MAAP): Assessing risk in complex environments*. Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Alexander, C. (2003). *Operational risk: Regulation, analysis and management*. London: FT Prentice Hall.

Allen, J. (2001). *The CERT ® Guide to system and network security practices*. Boston: Addison-Wesley.

Ames, M. (2005). *Untangling the net: Risk management for the enterprise*. Oslo: ISACA 33rd Annual Meeting Proceedings.

Amoroso, E. (1994). *Fundamentals of computer security*. Upper Saddle River: Prentice Hall PTR.

ASOSAI. (2003). *6th ASOSAI research project: IT audit guidelines*. New Delhi: The Asian Organisation of Supreme Audit Institutions (ASOSAI).

Bae, B., Epps, R. W. & Gwathmey, S. S. (2003). Internal control issues: the case of changes to information processes. *Information Systems Control Journal, 4*, 44-46.

Baki, L. & Rajczy, P. & Temesvari, M. (2004). *Assessing and managing operational risks at the Magyar Nemzeti Bank*. Budapest: Magyar Nemzeti Bank.

Barach, P. & Small, S. D. (2000). Clinical review - reporting and preventing medical mishaps: Lessons from non-medical near-miss reporting systems. *British Medical Journal, 320*, 759-763.

Barth, J. R., Caprio, Jr. G. & Levine, R. (2001a). *Banking systems around the globe: Do regulations and ownership affect performance and stability*. Chicago: University of Chicago Press.

Barth, J. R., Caprio, Jr. G. & Levine, R. (2001b). *The regulation and supervision of banks around the world: A new database*. Washington D.C.: Brookings Institution Press.

Barth, J. R., Caprio, Jr. G. & Levine, R. (2002). Bank regulation and supervision: What works best? *National Bureau of Economic Research Working Paper Series, 9323.*

Basel Committee. (2001a). *The new Basel Capital Accord: an explanatory note*. Basel: The Bank for International Settlements.

Basel Committee. (2001b). *Consultative document: operational risk*. Basel: The Bank for International Settlements.

Basel Committee. (2001c). *Working paper on the regulatory treatment of operational risk*. Basel: The Bank for International Settlements.

Basel Committee. (2001d). *Sound practices for the management and supervision of operational risk*. Basel: The Bank for International Settlements.

Basel Committee. (2002a). *Sound practices for the management and supervision of operational risk*. Basel: The Bank for International Settlements.

Basel Committee. (2002b). *Overview paper for impact study*. Basel: The Bank for International Settlements.

Basel Committee. (2002c). *About the Bank for International Settlements, Basel Committee on Banking Supervision*. Basel: The Bank for International Settlements.

Basel Committee. (2003a). *Sound practices for the management and supervision of operational risk*. Basel: The Bank for International Settlements.

Basel Committee. (2003b). *The New Basel Capital Accord consultative document*. Basel: The Bank for International Settlements.

Basel Committee. (2004). *International convergence of capital measurement and capital standards: A Revised Framework*. Basel: The Bank for International Settlements.

BBA, ISDA, RMA & PwC. (1999). *Operational risk: the next frontier*. Philadelphia: British Bankers' Association, the International Swaps and Derivatives Association, Risk Management Association, and PricewaterhouseCoopers.

Beaumaster, S. (2002). *Local government IT implementation issues: a challenge for public administration*. Hawaii: Proceedings of Hawaii International Conference on System Sciences.

Benjamin, R., Gladman, B. & Randell, B. (1998). Protecting IT systems from cyber crime. *The Computer Journal, 41/7*, 429-443.

Bernstein, T. (1996). *Internet security for business.* New York: John Wiley & Sons.

Bird, Jr. F. E. & Germain, G. L. (1996). *Practical loss control leadership*. Verias: Det Norte.

Bornman, W. G. & Labuschagne, L. (2006). *A comparative framework for evaluating information security risk management methods.* Auckland Park: Rand Afrikaans University.

Brag, V. & Wedefelt, F. (2004). *Information risk management*. Gothenburg: School of Economics and Commercial Law, Göteborg University.

BRSA. (2001). Regulation on banks' internal control and risk management systems – Banking Regulation and Supervision Agency. *Turkish Official Gazette, 8 February 2001*, 24312.

BRSA. (2006a). *An attitude of Banking Regulation and Supervision Agency for IT assurance*. Istanbul: IT Audit 2006 Workshops Proceedings.

BRSA. (2006b). Regulation on information systems assurance in the banks - Banking Regulation and Supervision Agency. *Turkish Official Gazette, 16 May 2006*, 26170.

BSI. (1999). *British Standard: Information security management part1 & part2*. London: British Standards Institute Group (BSI).

Buchanan, B., Arnold, T. & Nail, L. (2002). *Beware the ides of march: The collapse of HIH insurance*. Denver: 2003 FMA Conference Proceedings.

Buchanan, B. & Netter, J. (2002). *Money laundering and the Bank of New York*. New York: Terry College of Business, University of Georgia Working Papers.

Cagan, P. (2001). *Standard operating procedures*. Retrieved March 30, 2006, from http://www.erisk.com.

Campbell, P. L. (2003). *An introduction to information control models*. New Mexico: Sandia National Laboratories.

Carey, M. & Stulz, R. M. (2005). *The risks of financial institutions*. Columbus: Ohio State University Press.

Carr, M. (1993). *Taxonomy-based risk identification.* Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Chapelle, A. (2004). *Basel II and operational risk: Implications for risk measurement and management in the financial sector: Efficiency and stability in an evolving financial system.* Brussels: BNB-NBB Conference Working Papers.

Chapelle, A. (2005a). *Le risque opérationnel: Implications de l'Accord de Bâle pour le secteur financier*. Brussels: Edition Larcier.

Chapelle, A. (2005b). *The virtues of operational risk management*. Brussels: Université Libre de Bruxelles.

Charette, R. N. (1989). *Software engineering risk analysis and management.* New York: McGraw-Hill.

Chartis. (2006). *Operational risk management systems*. London: Chartis Research Ltd.

Colbert, J. L. & Bowen, P. L. (1996). A comparison of internal controls: COBIT, SAC, COSO and SAS55/78. *IS Audit & Control Journal, 4,* 26-35.

COSO. (1992). *Internal Control – Integrated Framework.* Washington: The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

COSO. (2004). *Enterprise Risk Management – Integrated Framework*. Washington: The Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Crouhy, C., Galai, D., & Mark, R. (2000). *Risk management.* New York: McGraw Hill.

Cruz, M. G. (2002). *Modeling, measuring and hedging operational risk.* New York: Wiley Finance.

Culp, C. (2001). *The risk management process: Business strategy and tactics*. New York: John Wiley & Sons.

Cumming, C. & Hirtle, B. (2001). The challenges of risk management in diversified financial companies. *FRBNY Economic Policy Review, March 2001*, 1-17.

Datardina, M. (2005). *Comparative analysis of IT control frameworks in the context of SOX*. Ontario: Centre for Information Systems Assurance, University of Waterloo.

Davidson, S. (2006). *The role of identity management: Moving from compliance to improved business performance*. New York: Computer Associates International, Inc.

Dellit, C. (2002). Governance and the emerging salience of technology. *Software, October 2002*, 19-24.

Di Renzo, B. & Bernard, C. (2005). *Operational risk management in financial institutions: Process assessment in concordance with Basel II*. Luxembourg: Centre de Recherche Public Henri Tudor & Commission de Surveillance du Secteur Financier.

Diebold, F. X., Schuermann, T. & Stroughair, J. D. (2000). Pitfalls and opportunities in the use of extreme value theory in risk management. *The Journal of Risk Finance, 1/2*, 30-36.

Donnelly, P. (2001). What every audit committee member should know. *The RMA Journal, September 2001*, 48-51.

Dowd, W. (2001*). Insurance of operational risk and the New Basel Capital Accord.* Boston: Capital Allocation for Operational Risk Conference Proceedings.

Dorofee, A. J. (1996). *Continuous risk management guidebook*. Pittsburg: Software Engineering Institute, Carnegie Mellon University.

Embrechts, P., Klueppelberg, C. & Mikosch, T. (1997): *Modelling external events*. Berlin: Springer.

EU. (2006a). *Capital Requirements Directive.* Brussels: European Union.

EU. (2006b). *Statutory Audit Directive.* Brussels: European Union.

Federal Reserve Bank of Boston. (2001). *Notes about the conference on capital allocation for operational risk.* Boston: Federal Reserve Bank of Boston.

Filipovic, D. & Rost, D. (2006). *Benchmarking study of internal models.* Amsterdam: The Chief Risk Officer Forum.

Frachot, A., Georges, P. & Roncalli, T. (2001): *Loss distribution approach for operational risk*. Lyon: Groupe de Recherche Opérationnelle Working Papers, Crédit Lyonnais.

Frachot, A., Georges, P. & Roncalli, T. (2002): *Mixing internal and external data for managing operational risk*. Lyon: Groupe de Recherche Opérationnelle Working Papers, Crédit Lyonnais.

Gallagher, B. (1999). *Software acquisition risk management key process area (KPA) – A guidebook version 1.02*. Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Garfinkel, S. & Spafford, G. (1996). *Practical UNIX and internet security second edition*. Sepastopol: O'Reilly & Associates, Inc.

GIRO. (2002). *Operational risk: Report of the operational risks working party*. Arlington: General Insurance Research Organization (GIRO).

Goldstein, M. (2001). *Comment and discussion on relevance and the need for international regulatory standards*. Washington D.C.: Brookings Institution Press.

Grembergen, W. V. (2000). The balanced scorecard and IT governance. *Information Systems Control Journal, 2.*

Group of Thirty. (1993). *Derivatives: practices and principles*. Washington: Group of Thirty.

Guldentops, E. (2002). Knowing the environment: top five IT issues. *Information Systems Control Journal, 4*, 15-16.

Haimes, Y. Y. (2004). *Risk modeling, assessment, and management*. New York: John Wiley & Sons, Inc.

Hamaker, S. (2003). Spotlight on governance. *Information Systems Control Journal, 1*, 15-19.

Hardy, G. (1995). *Standards - The need for a common framework.* London: Proceedings of COMPSEC International 1995, 12th World Conference on Computer Security, Audit and Control.

Hardy, G. (2002). Make sure management and IT are on the same page: implementing an IT Governance framework. *Information Systems Control Journal, 3*, 14-16.

Harris, R. (2002a). *Emerging practices in operational risk management*. Chicago: Federal Reserve Bank of Chicago.

Harris, R. (2002b). *A domestic regulatory approach to operational risk*. Chicago: Federal Reserve Bank of Chicago.

Herring, R. J. (2002). *The Basel 2 approach to bank operational risk: Regulation on the wrong track.* Philadelphia: University of Pennsylvania.

Hiwatashi, J. (2002). *Solutions on measuring operational risk*. Chicago: Capital Markets News, the Federal Reserve Bank of Chicago.

Hoffman, D.G. (2002). *Managing operational risk: 20 firmwide best practice strategies*. New York: Wiley Frontiers in Finance, John Wiley & Sons, Inc.

Hoffmann, T. (2003). Sidebar: Guidelines meld IT governance: Sarbanes-Oxley compliance. *Computerworld, July 2003*.

Howard, J. D. & Longstaff, T. A. (1998). A common language for computer security incidents. *SAND98-8667, October 1998*.

ISACA. (2006). *CISA review manual 2007*. Rolling Meadows: Information Systems and Control Association (ISACA).

ISDA. (2000). *A new capital adequacy framework: Comments on a consultative paper issued by the Basel Committee on Banking Supervision in June 1999*. New York: International Swaps and Derivatives Association, Inc.

ISO. (2005). *Information technology – Security techniques - Information security management systems – Requirements*. Geneva: International Organization for Standardization (ISO).

ITGI. (2000). *COBIT® 3rd edition.* Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2003). *Board briefing on IT governance.* Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2004). *IT control objectives for Sarbanes-Oxley 1st edition: The Importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting*. Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2005). *COBIT® 4th edition.* Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2006a). *COBIT® mapping: Mapping of ISO/IEC 17799:2005 with COBIT® 4.0.* Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2006b). *IT control objectives for Sarbanes-Oxley 2nd edition: The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting*. Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2007a). *COBIT® mapping: Mapping of ITIL® with COBIT® 4.0.* Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2007b). *IT control objectives for Basel II: The importance of governance and risk management for compliance (draft exposure)*. Rolling Meadows: IT Governance Institute (ITGI).

ITGI & PwC. (2004). *IT governance global status report 2003*. Rolling Meadows: IT Governance Institute (ITGI) & PricewaterhouseCoopers (PwC).

ITGI & PwC. (2006). *IT governance global status report 2005*. Rolling Meadows: IT Governance Institute (ITGI) & PricewaterhouseCoopers (PwC).

Jochum, C. (2006). *IT risk management in the banking industry*. Frankfurt am Main: Institut für Wirtschaftsinformatik.

Jones, S., Kirchsteiger, C. & Bjerke, W. (1999). The Importance of near miss reporting to further improve safety performance. *Journal of Loss Prevention in the Process Industries, 12,* 59-67.

Kane, E. J. (2001). *Relevance and the need for international regulatory standards.* Washington: Brookings Institution Press.

King, J. L. (1998). Defining operational risk. *ALGO Research Quarterly, 1/2*, 37-42.

King, J. L. (2001). *Operational risk*. New York: John Wiley & Sons.

Kloman, H. F. (1990). Risk management agonists. *Risk Analysis, 10/2*, 201-205.

Korac-Kakabadse, N. & Kakabadse, A. (2001). IS/IT governance: need for an integrated model. *Corporate Governance, 1/4,* 9-11.

Kuritzkes, D. R. (2002). *Operational risk poses challenges to financial institutions and regulators*. Philadelphia: Wharton Financial Institutions Center.

Kvistad, J. & Donnelly, P. (2001). An examiner's view of operational risk. *Bank News, June 2001*.

Lainhart, J. W. (2000). Aligning IT controls with business objectives is crucial to sustained enterprise success. *EDPACS, 28/4*, 1-11.

Lainhart, J. W. (2001). *COBIT management guidelines IT governance forum trust and understanding for the business and the board.* Paris: ITGI Paris.

Lanz, J. (2002). Prioritizing aspects of technology risk assessment and mitigation. *Bank Accounting & Finance, December 2002*, 19-26.

Loewenton, I. (2003). *Mastering and managing operational risks in banking and financial institutions & Basel II New Accord for operational risks*. Lausanne: École Des Hautes Études Commerciale Université De Lausanne.

Lindqvist, U. & Jonsson, E. (1997). *How to systematically classify computer security intrusions.* Oakland: Proceedings of IEEE Symposium on Security and Privacy.

Liu, Q. & Ridley, G. (2006). *IT control in the Australian public sector: An international comparison*. Sandy Bay: University of Tasmania.

Machin, J. (2002). *The ABCs of corporate governance.* New York: KPMG LLP.

Marshall, C. (2001). *Measuring and managing operational risk in financial institutions: Tools, techniques and other resources.* Singapore: John Wiley & Sons, Inc.

Marshall, C. & Heffes, E. M. (2003). Study faults bank risk management. *Financial Executive, 19/9*.

Mazıbaş, M. (2005). *Operasyonel riske Basel yaklaşımı: Risk verilerine ilişkin bir değerlendirme*. Ankara: Bankacılık Düzenleme ve Denetleme Kurulu (BDDK).

Mc Connell, P. (2005). *Measuring operational risk management systems under Basel II*. Sydney: Risk Trading Technology.

Musson, D. & Jordan, E. (2004). *The broken link: Corporate governance and information technology*. Sydney: Macquarie Graduate School of Management**.**

Mürmann, A. (2002). *Operational risk poses challenges to financial institutions and regulators*. Philadelphia: Wharton Financial Institutions Center.

Mürmann, A. & Öktem, Ü. (2002). *The near-miss management of operational risk.* Philadelphia: University of Pennsylvania.

Nash, M., Nakada, P. & Johnston, B. (2002). Start today for enterprise-wide risk management in 2006. *The RMA Journal, November 2002*, 56-61.

Netter, J. M. & Poulsen, A. B. (2005). *Operational risk in financial service providers and the proposed Basel Capital Accord: An overview*. Athens: University of Georgia.

Neumann, P. G. & Parker, D. B. (1989). *A summary of computer misuse techniques.* Baltimore: Proceedings of the 12th National Computer Security Conference.

Norris, V. A. & Young, L. R. (2005). *Risk assessment in Sarbanes-Oxley*. Charleston: Advanced Technology Institute.

OGC. (2004). *Information Technology Infrastructure Library v.2*. Norwich: The Office of Government Commerce (OGC).

Panko, R. R. (2006). *Spreadsheets and Sarbanes-Oxley: Regulations, risks, and control frameworks*. Hawaii: University of Hawaii.

Payne, N. (2003). IT Governance and audit. *Accountancy SA, January 2003*, 35.

Perry, S. (2004). The Sarbanes-Oxley Act: Opportunities for e-Business. *E-Business Review, Fall 2004*, 54-63.

Perry, T. & Wallich, P. (1984). Can computer crime be stopped? *IEEE Spectrum, 21/5*.

Petrou, K. S. (2002). *Taking care with capital rules: Why getting them right matters so much*. Washington: Federal Financial Analytics, Inc.

Phimister, J. R. (2001a). *Near-miss management systems in the chemical process industry*. Philadelphia: Wharton Risk Management and Decision Processes Center, University of Pennsylvania.

Phimister, J. R. (2001b). *Statistical, analytical and management tools for near-miss programs.* Philadelphia: Wharton Risk Management and Decision Processes Center, University of Pennsylvania.

Pipkin, D. L. (2000). *Information security: Protecting the global enterprise.* Upper Saddle River: Prentice-Hall PTR.

Putnam, A. H. (2004). *Information security management references*. Washington: United States House of Representatives

RMG. (2002). *The quantitative impact study (QIS) for operational risk: Overview of individual loss data and lessons learned: Report to Basel Committee.* Basel: Risk Management Group, Bank for International Settlements.

Rosengren, E. (2002). *Quantification of operational risk*. Chicago: Presentations at FRB of Chicago Bank Structure Conference.

Samad-Khan, A. (2005). *Why COSO is flawed?* Retrieved January 18, 2005, from http://www.operationalriskonline.com

Saunders, A. (2000). *Financial institutions management: A modern perspective.* New York: McGraw Hill.

Schneider, F. B. (1999). *Trust in cyberspace.* Washington: National Academy Press.

SEI. (2002) *Capability Maturity Model® Integration (CMMI), version 1.1*. Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Sharp, A. & Mc Dermott, P. (2001). *Workflow modeling: Tools for process improvement and application development.* Boston: Artech House.

Shortreed, J., Hicks, J. & Craig, L. (2003). *Basic frameworks for risk management*. Ontario: The Ontario Ministry of the Environment.

Smith, H. A., Mc Keen, J. D. & Staples, D. S. (2001). Risk management in information systems: Problems and potentials. *Communications of AIS, 7*, 13 21.

TBB. (2004). Operasyonel risk veri tabanı. *Türkiye Bankalar Birliği (TBB) Bankacılar Dergisi, 50*, 84-130.

Thornhill, W. T. (1990). *Risk management for financial institutions.* New York: Bankers Publishing Company.

Tyler, R. (2000). Implementing COBIT in New South Wales Health. *Information Systems Control Journal, 3*, 30-32.

USC. (2002). *Sarbanes-Oxley Act*. Washington: United States Congress.

Warland, C. & Ridley, G. (2005). *Awareness of IT control frameworks in an Australian state government: A qualitative case study*. Hawaii: Proceedings of the 38th Hawaii International Conference on System Sciences.

Williams, R. C. (1999). *Software risk evaluation (SRE) method description version 2.0.* Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

Wood, C. C. (2001). *Best practices in internet commerce security.* Houston: PentaSafe Security Technologies, Inc.

Young, P. C. & Tippins, S. C. (2001). *Managing business risk: An organization-wide approach to risk management.* New York: American Management Association.

REFERENCES NOT CITED

ACERT. (1995). *UNIX computer security checklist version 1.1*. Sidney: Australian Computer Emergency Response Team.

AFSL. (2003). *Operational risk: The last of the risk frontiers? An operational & technical framework*. London: Amelia Financial Systems Limited (AFSL).

AICE. (1992). *Guidelines for investigating chemical process incidents*. New York: Center for Chemical Process Safety, American Institute for Chemical Engineers.

Allen, J. (2001). *Presentation on information security as an institutional priority.* Pittsburgh: Carnegie Mellon University.

BEMA. (2006). *Banks and deposit companies: The management of operational risk*. Bermuda: The Bermuda Monetary Authority (BEMA).

Brewer, D. (1998). *Les criteres d'homologation de la securite des systemes d'information*. Paris: Eurosec 1998 Conference Proceedings.

Buckby, S., Best, P. & Stewart, J. (2006).*The role of boards in reviewing information technology governance (ITG) as part of organizational control environment assessments.* Brisbane: Queensland University of Technology.

Caouette, J. B., Altman, E. I. & Narayanan, P. (1998). *Managing credit risk: The next great financial challenge*. Toronto: Wiley Frontiers in Finance, John Wiley & Sons, Inc.

Chung, C. (2003). *Information system environment for the operational risk management*. Paris: Ecole des Mines de Paris.

Ciborra, C. (2004). *Discussion paper on digital technologies and the duality of risk.* London: Centre for Analysis of Risk and Regulation The London School of Economics and Political Science.

Clark, D. C. (1991). *Computers at risk: Safe computing in the information age*. Washington: National Academy Press.

Cohen, F. B. (1995). Viruses, corruption, denial, disruption, and information assurance. *Information Security - the Next Decade, May 1995*, 495-509.

Crosby, P. B. (1979). *Quality is free: The art of making quality certain*. New York: McGraw-Hill.

Cummins, J. D., Lewis, C. M. & Wei, R. (2004). *The market value impact of operational risk events for U.S. banks and insurers*. Philadelphia: University of Pennsylvania.

Currie, C. (2004). *Potential effects of the new Basel operational risk capital requirements*. Sydney: University of Technology.

Currie, C. (2005). *A test of the strategic effect of Basel II operational risk requirements on banks*. Sydney: University of Technology.

Curry, D. A. (1990). *Improving the security of your UNIX system*. Menlo Park: SRI International.

Danielsson, J. (2000). *The emperor has no clothes: Limits to risk modelling*. London: Special Paper Series No. 126, Financial Markets Group, London School of Economics.

Danielsson, J. (2001). *An academic response to Basel II.* London: Special Paper Series No. 130, Financial Markets Group, London School of Economics.

De Bie, C. (2006). *Exploring ways to model reputation loss*. Rotterdam: Erasmus University.

De Fontnouvelle, P. (2003). *Using loss data to quantify operational risk*. Boston: Federal Reserve Bank of Boston.

Deming, W. E. (1986). *Out of the crisis*. Cambridge: Center for Advanced Engineering Study, Massachusetts Institute of Technology.

Di Renzo, B., Feltus, C. & Prime, S. (2004). *Collaborative management for ICT process improvement in SME: experience report*. Luxembourg: Centre de Recherche Public Henri Tudor.

Dingle, J. F. (2001). *The elements of the global network for large-value funds transfers*. Ottawa: Bank of Canada.

DTI. (1993). *A code of practice for information security management*. London: Department of Trade and Industry & British Standard Institute.

Embrechts, P. (2002). *Extremes in economics and the economics of extremes.* Zurich: Swiss Federal Institute of Technology.

Embrechts, P., Kaufmann, R. & Samorodnitsky, G. (2004). *Ruin theory revisited: Stochastic models for operational risk*. Zurich: Swiss Federal Institute of Technology.

Faisst, U. & Prokein, O. (2006). *Management of security risks - a controlling model for banking companies*. Augsburg: Universität Augsburg.

FFIEC. (2003). *IT examination handbook*. Washington: Federal Financial Institutions Examination Council (FFIEC).

Fitzgerald, J. & Fitzgerald, A. F. (1990). Designing controls into computerized systems. Redwood City: Jerry FitzGerald and Associates.

Friesenecker, S. (2005). *Management presentation on IT governance and SOX*. New York: UBS Group.

Glaessner, T., Kellermann, T. & Mc Nevin, V. (2002). *Electronic security: Risk mitigation in financial transactions*. New York: The World Bank.

GAO. (2001). *Management planning guide for information systems security auditing*. Washington: National State Auditors Association and the U. S. General Accounting Office (GAO).

Gaston, S. J. (1996). *Information security - Strategies for successful management.* Toronto: The Canadian Institute of Chartered Accountants.

George, M. L. (2003). *Lean six sigma For Service*. New York: McGraw Hill.

Gewald, H. & König, W. (2004). *Role of perceived risk and technology acceptance.* Frankfurt am Main: Institut für Wirtschaftsinformatik.

Guldiman, T. (2001). *Capital allocation for operational risk*. Boston: Credit Suisse Group.

Hayden, T. & Schablik, P. (2001). *Information technology risk assessment*. Boston: Proceedings of Annual Conference & Expo on Control and Audit of Information Technology.

Hélie, S. G. (2000). *Sécurité internet*. Paris: Dunod.

Hélie, S. G. (2002). *Internet et sécurité: Que sais-je.* Paris: Puf.

Helle, A. J. (2005). Security culture and risk management is a management responsibility. *Telektronikk, 1.*

Herring, R. J. (1999). Credit risk and financial instability. *Oxford Review of Economic Policy, 15/3*, 63-79.

Herring, R. J. (2002). The regulation of operational risk in investment management companies. *Perspective, 8/2*, 1-19.

Herring, R. J. (2003). *International financial conglomerates: Implications for bank insolvency regimes.* Philadelphia: University of Pennsylvania.

Hesse, M. & Pohlmann, N. (2006). Wertschöpfung oder bedrohung für das unternehmen? *IT-Sicherheit, 5/2006.*

Howard, J. D. (1997). *An analysis of security incidents on the internet, 1989-1995*. Pittsburgh: Carnegie Mellon University.

Hubbard, L. (2001). *Control self-assessment: A practical guide*. Altamonte Springs: The Institute of Internal Auditors.

Humphrey, W. S. (1988). Characterizing the software process, *IEEE Software, 5/2*, 73-79.

Hunter, S., Kobelsky, K. & Richardson, V. J. (2003). Information technology and the volatility of firm performance. *MIT Sloan School of Management Working Paper, November 2003*.

IIA. (1998). *Professional Practices Pamphlet 98-2: A perspective on control self-assessment*. Altamonte Springs: The Institute of Internal Auditors.

INTOSAI. (2002). System development audit. *International Organization of Supreme Audit Institutions, Into IT Journal, 16*.

INTOSAI. (2004). *An INTOSAI IT audit committee project: CAATs for non-financial audit*s. Sultanate of Oman: International Organization of Supreme Audit Institutions.

ISAICAI. (2004). IT/ IS audit standards. *The Institute of Chartered Accountants of India, IT Harmony, 2/12*.

ITGI. (2003). *Information security governance: Guidance for boards of directors and executive management*. Rolling Meadows: IT Governance Institute (ITGI).

ITGI, (2005). *Aligning CobiT, ITIL, and ISO17799 for business benefit: Management summary*. Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2006). *CobiT mapping: Overview of international IT guidance 2nd edition.* Rolling Meadows: IT Governance Institute (ITGI).

ITGI. (2007). *CobiT mapping: Mapping of CMMI for development v1.2. with CobiT 4.0.* Rolling Meadows: IT Governance Institute (ITGI).

Julian, T. (2006). *Database auditing best practices*. New York: Application Security Inc.

Kellogg, P. (2003). *Evolving operational risk management for retail payments*. Chicago: Federal Reserve Bank of Chicago.

Kersten, B. & Verhoef, C. (2003). *IT portfolio management: A banker's perspective on IT*. Cutter IT Journal, 16/4.

Kirstein, R. (2002). The new Basel Accord, internal ratings, and the incentives of banks. *International Review of Law and Economics, 21*, 393-412.

Kleindorfer, P., Kunreuther, H. C. & Schoemaker, P. J. H. (1993). *Decision sciences: An integrative perspective.* New York: Cambridge University Press.

Kraft, E. (2002). *Working papers on foreign banks in Croatia: Another look.* Zagreb: Croatian National Bank.

Krainer, R. (2002). Banking in a theory of the business cycle: a model and critique of the Basel Accord on risk-based capital requirements for banks. *International Review of Law and Economics, 21*, 413-433.

Krasavin, S. (2006). *Auditing Windows web server IIS5.0 with free tools: An auditing perspective.* Chicago: University of Illinois.

Krasniqi, V. (2004). *Umsetzung des IT-risikomanagements bei banken*. Zürich: Institut für Informatik der Universität Zürich.

Krauss, L. I. (1980). *SAFE: security audit and field evaluation for computer facilities and information systems*. New York: Amacom.

Kupper, E. F. (2002). *Risk management in banking.* Sydney: Australian Prudential Regulation Authority (APRA).

Lam, J. (2006). *The impacts and implications of ERM on IT.* San Francisco: OCEG IT Forum Conference.

Larsen, M. H., Pedersen, M. K. & Andersen, K. V. (2006).*IT governance: Reviewing 17 IT governance tools and analysing the case of Novozymes A/S.* Hawaii: Proceedings of the 39th Hawaii International Conference on System Sciences.

Le Grand, C. H. (2001). *IT audit forum: Information technology in auditing*. Altamonte Springs: The Institute of Internal Auditors.

Levine, D. E. (1995a). *Auditing computer security*. New York: John Wiley & Sons, Inc.

Levine, D. E. (1995b). EDP auditing and related packages. New York: John Wiley & Sons, Inc.

Lillywhite, T. (1999). How to protect your information: an introduction to BS7799. *Management Services, January 1999*, 20-21.

Mc Connell, P. & Blacker, K. (2000). *An approach to modelling operational risk in banks*. Oxon: Henley Management College.

Meadows, C. (1992). *An outline of a taxonomy of computer security research and development*. Little Compton: Proceedings of the 1992-1993 ACM Workshop on New Security Paradigms.

Megginson, W. & Netter, J. (2001). From state to market: A survey of empirical studies on privatization. *Journal of Economic Literature, 39*, 321-389.

Miers, D. (2004). *Balancing efficiency and agility*. London: Enix Consulting Business Process Management Group.

Mitra, G. (2005). *SOXA: The why's, when's and how's?* London: School of Information Systems, Computing & Mathematics, Brunel University.

Mitre. (1999). *Defense-information assurance red team methodology*. Bedford: Mitre Corporation.

NIST. (1995). *An introduction to computer security: The NIST handbook.* Gaithersburg: National Institute of Standards and Technology.

NIST. (2001). *Federal information technology security assessment framework.* Gaithersburg: National Institute of Standards and Technology.

NIST. (2002). *Risk management guide for information technology systems.* Gaithersburg: National Institute of Standards and Technology.

OECD. (1992). *Guidelines for the security of information systems.* Paris: Organization for Economic Cooperation and Development.

Oliver, D. J. (1999). Is your business c:cure? *IS Audit & Control Journal, 6/1999*, 23-26.

Opausky, M. (2006). *Technology supporting the convergence of governance, risk & compliance.* New York: 7th Annual GARP Conference Proceedings.

Pariwat, S. & Hataiseree, R. (2003). *2nd SEACEN-CPSS course on the PSS for emerging economies: Managing payment and settlement system reform (A Thai perspective).* Bangkok: Banka of Thailand Payment Systems Group.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. New York: John Wiley & Sons.

Parkin, R. (1995). *IT security - An implementation strategy*. London: Proceedings of COMPSEC International 95, 12th World Conference on Computer Security, Audit and Control.

Raff, D. M. G. (2001). *Risk management in an age of change.* Philadelphia: University of Pennsylvania.

Rapalus, P. (2001). CSI/FBI computer crime and security survey. *Computer Security Journal, November 2001*, 29-51.

Rasmussen, M. & Stamp, P. (2005). *IT's role in enterprise risk management.* Cambridge: Trends, Forrester Research, Inc.

Rivest, R. L. (1998). *Chaffing and winnowing: Confidentiality without Encryption*. Massachusetts: MIT Lab for Computer Science.

Rodewald, G. (2005). *Aligning information security investments with a firm's risk tolerance.* Kennesaw: Kennesaw State University.

Roth, J. (1997). *Control model implementation: Best practices*. Altamonte Springs: The Institute of Internal Auditors Research Foundation.

Ruthberg, Z. G. (1988). *Guide to auditing for controls and security: A System Development Life Cycle*. Gaithersburg: National Institute of Standards and Technology.

Saaty, T.L. (2001). *Decision making for leaders*. Shallowater: RWS Publications.

Schneier, B. (2000). Risks of relying on cryptography. *Inside Risks Column, 42/10*, 144.

Scholtes, P. R. (1994). *The team handbook: How to use teams to improve quality.* Oklahoma: Joiner Associates, Inc.

Sheedy, E. (1999). *Applying an agency framework to operational risk management.* Sydney: Macquarie University.

Solms, B. V. (2005). *Information security governance: COBIT or ISO 17799 or both?* Johannesburg: Academy for Information Technology, University of Johannesburg.

SPK, 2003). *Kurumsal yönetim ilkeleri*. Ankara: Sermaye Piyasası Kurulu (Capital Market Committee).

Stephenson, P. (2006). *Standards-traceable reference architecture for information systems: A method for security requirements engineering using a standards-based network security reference model.* Oxford: Oxford Brookes University.

Stoneburner, G. (2001). *Engineering principles for information technology security: A baseline for achieving security.* Gaithersburg: National Institute of Standards and Technology.

Swanson, M. & Guttman, B. (1998). *Guide for developing security plans for information technology systems*. Gaithersburg: National Institute of Standards and Technology.

Swanson, M. (2001). *Security self-assessment guide for information technology systems*. Gaithersburg: National Institute of Standards and Technology.

Szakats, D. (2004). *IT maturity and sourcing strategies*. Zürich: Institut für Informatik der Universität Zürich.

Tarantino, A. (2005). Global compliance initiatives and the risk and IT standards to support them. *Enterprise Risk Management and Governance Advisory Service Executive Update, 2/11*, 1-4.

TBJ. (2001). *Technological innovation and banking industry/monetary policy: Forum on the development of electronic payment technologies and its implications for monetary policy*. Tokyo: The Bank of Japan.

Teker, D. L. & Ülengin, B. (2005). Bankacılıkta operasyonel risk ölçüm modellerinin Türk bankacılık sektöründe faaliyet gösteren bir bankaya uygulanması. *İTÜ Dergisi Sosyal Bilimler, 2/1*, 13-24.

Tipton, H. F. & Krause, M. (2000). *Information security management handbook, 4th edition.* Boca Raton: CRC Press.

Tripp, M. H, Bradly, H. L. & Devitt, R. (2003). *Risk measurement or bust*. Arlington: General Insurance Research Organization (GIRO).

Tripp, M. H, Bradly, H. L. & Devitt, R. (2004). *Quantifying operational risk in general insurance companies*. Reigate: Watson Wyatt LLP.

Troy, E. F. (1998). *Common Criteria: Launching the international standard*. Gaithersburg: National Institute of Standards and Technology.

Vallabhaneni, S. R. (1989). *Auditing computer security.* New York: John Wiley & Sons, Inc.

Volders, G. (2004). *How to use CobiT to assess the security & reliability of digital preservation*. Antwerp: Erpa Workshop.

Watangase, T. (2005). *2nd SEACEN Federal Reserve System Course on Electronic Banking and Technology Risk Supervision: Supervisory Concerns in an IT Environment*. Bangkok: Banka of Thailand Payment Systems Group.

Wei, R. (2003). *Operational risks in the insurance industry*. Philadelphia: University of Pennsylvania.

Wildhaber, B. (2003). *IT governance: Critical success factors.* Thalwil: ZFU International Business School.

Wilmarth, A. E. (2002). *Controlling systemic risk in an era of financial consolidation.* Washington: George Washington University.

Wood, C. C. (1987). *Computer security: A comprehensive controls checklist*. New York: John Wiley & Sons.

Wood, C. C. (1990). Principles of secure information systems design. *Computers & Security, 9*, 13-24.

APPENDIX A

WORKSHOP PARTICIPANTS

Assist. Prof. Ceylan Onay

Boğaziçi University, Department of Management Information Systems, Instructor

Dr. Tamer Şıkoğlu

Boğaziçi University, Department of Management Information Systems, Instructor

Ernst & Young, Technology and Risk Services, Manager

Assoc. Prof. Birgül Kutlu

Boğaziçi University, Department of Management Information Systems, Instructor

Tumin Gültekin

PricewaterhouseCoopers Turkey, System & Process Assurance, Senior Manager (CISA)

Serdar Güzel

PricewaterhouseCoopers Turkey, System & Process Assurance, Assist. Manager (CISA)

Güçlü Şeneler

Opet Petrolcülük A. Ş., Internal Audit Department, Department Head

APPENDIX B

CONTROL OBJECTIVE MAPPING DETAILS

Table 19: Mapping Legend

Context	Item	Symbol
Operational Risk Categories	Internal Fraud	1
	External Fraud	2
	Employment Practices and Workplace Safety	3
	Clients, Products & Business Practices	4
	Damage to Physical Assets	5
	Business Disruption and System Failures	6
	Execution, Delivery & Process Management	7
Control Types	Preventive	P
	Detective	D
	Corrective	C

Table 20: Mapping Results

Detailed Control Objective in CobiT	Proposed Mapping	Workshop Result	Consensus on Mapping in the Workshop
PO1.1 IT Value Management	4-P	4-P	OK
PO1.2 Business-IT Alignment	4-P	4-P	OK
PO1.3 Assessment of Current Performance	7-D	7-D	OK
PO1.4 IT Strategic Plan	4-P	4-P	OK
PO1.5 IT Tactical Plans	4-P	4-P	OK
PO1.6 IT Portfolio Management	6-P	4-P	OK
PO2.1 Enterprise Information Architecture Model	6-P	4-P	OK
PO2.2 Enterprise Data Dictionary and Data Syntax Rules	6-P	4-P	OK
PO2.3 Data Classification Scheme	6-P	4-P	OK
PO2.4 Integrity Management	6-P	4-P	OK
PO3.1 Technological Direction Planning	6-P	4-P	OK
PO3.2 Technological Infrastructure Plan	6-P	4-P	OK
PO3.3 Monitoring of Future Trends and Regulations	7-D	7-D	OK
PO3.4 Technology Standards	4-P	4-P	OK
PO3.5 IT Architecture Board	4-P	4-P	OK
PO4.1 IT Process Framework	4-P	4-P	OK
PO4.2 IT Strategy Committee	4-P	4-P	OK
PO4.3 IT Steering Committee	4-P	4-P	OK
PO4.4 Organizational Placement of the IT Function	3-P	3-P	OK
PO4.5 IT Organizational Structure	3-P	3-P	OK
PO4.6 Roles and Responsibilities	1-P	1-P	OK

PO4.7 Responsibility for IT Quality Assurance	7-D	7-P	6 times 7-P, once 7-D
PO4.8 Responsibility for Risk, Security and Compliance	4-P	1-P	OK
PO4.9 Data and System Ownership	4-P	1-P	OK
PO4.10 Supervision	4-P	4-P	OK
PO4.11 Segregation of Duties	1-P	1-P	OK
PO4.12 IT Staffing	3-D	3-P	OK
PO4.13 Key IT Personnel	1-P	7-P	OK
PO4.14 Contracted Staff Policies and Procedures	4-P	2-P	6 times 2-P, once 4-P
PO4.15 Relationships	3-P	3-P	OK
PO5.1 Financial Management Framework	4-P	4-P	OK
PO5.2 Prioritisation Within IT Budget	4-P	4-P	OK
PO5.3 IT Budgeting Process	4-D	4-D	OK
PO5.4 Cost Management	4-D	4-D	OK
PO5.5 Benefit Management	4-D	4-D	OK
PO6.1 IT Policy and Control Environment	4-P	4-P	OK
PO6.2 Enterprise IT Risk and Internal Control Framework	4-P	4-P	OK
PO6.3 IT Policies Management	4-P	4-P	OK
PO6.4 Policy Rollout	4-P	4-P	OK
PO6.5 Communication of IT Objectives and Direction	4-D	4-P	6 times 4-P, once 4-D
PO7.1 Personnel Recruitment and Retention	3-P	3-P	OK
PO7.2 Personnel Competencies	3-D	3-D	OK
PO7.3 Staffing of Roles	3-P	3-P	OK
PO7.4 Personnel Training	3-P	3-P	OK
PO7.5 Dependence Upon Individuals	3-P	3-P	OK
PO7.6 Personnel Clearance Procedures	3-P	1-P	OK
PO7.7 Employee Job Performance Evaluation	3-D	3-C	4 times 3-C, 3 times 3-D
PO7.8 Job Change and Termination	1-P	1-P	OK
PO8.1 Quality Management System	4-D	4-D	OK
PO8.2 IT Standards and Quality Practices	4-P	4-P	OK
PO8.3 Development and Acquisition Standards	4-P	4-P	OK
PO8.4 Customer Focus	7-P	7-P	OK
PO8.5 Continuous Improvement	4-C	4-C	OK
PO8.6 Quality Measurement, Monitoring and Review	7-D	7-D	OK
PO9.1 IT and Business Risk Management Alignment	4-P	4-P	OK
PO9.2 Establishment of Risk Context	4-P	4-P	OK
PO9.3 Event Identification	7-D	7-P	OK
PO9.4 Risk Assessment	4-C	4-D	OK
PO9.5 Risk Response	4-C	4-C	OK
PO9.6 Maintenance and Monitoring of a Risk Action Plan	7-D	7-D	OK
PO10.1 Programme Management Framework	6-P	4-P	OK
PO10.2 Project Management Framework	4-P	4-P	OK
PO10.3 Project Management Approach	4-P	4-P	OK
PO10.4 Stakeholder Commitment	7-D	4-P	OK

PO10.5 Project Scope Statement	4-P	4-P	OK
PO10.6 Project Phase Initiation	4-P	4-P	OK
PO10.7 Integrated Project Plan	4-P	4-P	OK
PO10.8 Project Resources	3-P	3-P	4 times 3-P, 3 times 7-P
PO10.9 Project Risk Management	7-P	7-D	OK
PO10.10 Project Quality Plan	4-P	4-P	OK
PO10.11 Project Change Control	7-D	7-P	OK
PO10.12 Project Planning of Assurance Methods	4-C	4-C	OK
PO10.13 Project Performance Measurement, Reporting and Monitoring	7-D	7-D	OK
PO10.14 Project Closure	7-C	7-C	6 times 7-C, once 7-P
AI1.1 Definition and Maintenance of Business Functional and Technical Requirements	4-P	4-P	OK
AI1.2 Risk Analysis Report	4-D	4-D	OK
AI1.3 Feasibility Study and Formulation of Alternative Courses of Action	4-C	4-P	OK
AI1.4 Requirements and Feasibility Decision and Approval	4-C	4-P	OK
AI2.1 High-level Design	4-P	4-P	OK
AI2.2 Detailed Design	4-P	4-P	OK
AI2.3 Application Control and Auditability	7-P	7-P	OK
AI2.4 Application Security and Availability	4-P	1-P	OK
AI2.5 Configuration and Implementation of Acquired Application Software	6-P	6-P	OK
AI2.6 Major Upgrades to Existing Systems	6-P	6-P	OK
AI2.7 Development of Application Software	6-D	6-D	OK
AI2.8 Software Quality Assurance	7-P	7-D	OK
AI2.9 Applications Requirements Management	7-C	7-D	OK
AI2.10 Application Software Maintenance	7-C	7-C	6 times 7-C, once 7-P
AI3.1 Technological Infrastructure Acquisition Plan	6-P	4-P	OK
AI3.2 Infrastructure Resource Protection and Availability	6-P	6-P	OK
AI3.3 Infrastructure Maintenance	6-P	6-P	OK
AI3.4 Feasibility Test Environment	1-P	6-P	OK
AI4.1 Planning for Operational Solutions	4-P	7-P	OK
AI4.2 Knowledge Transfer to Business Management	3-P	3-P	OK
AI4.3 Knowledge Transfer to End Users	3-P	3-P	OK
AI4.4 Knowledge Transfer to Operations and Support Staff	3-P	7-P	OK
AI5.1 Procurement Control	4-P	4-P	6 times 4-P, once 7-P
AI5.2 Supplier Contract Management	7-P	7-P	OK
AI5.3 Supplier Selection	7-P	7-P	OK
AI5.4 Software Acquisition	7-P	7-P	OK
AI5.5 Acquisition of Development Resources	7-P	7-P	OK
AI5.6 Acquisition of Infrastructure, Facilities and Related Services	7-P	7-P	OK
AI6.1 Change Standards and Procedures	4-P	4-P	OK

AI6.2 Impact Assessment, Prioritization and Authorization	1-P	6-P	OK
AI6.3 Emergency Changes	1-P	1-P	6 times 1-P, once 6-P
AI6.4 Change Status Tracking and Reporting	1-D	7-D	OK
AI6.5 Change Closure and Documentation	1-D	7-D	OK
AI7.1 Training	3-P	3-P	OK
AI7.2 Test Plan	7-C	7-P	OK
AI7.3 Implementation Plan	7-P	7-P	OK
AI7.4 Test Environment	7-D	7-P	OK
AI7.5 System and Data Conversion	6-P	6-P	OK
AI7.6 Testing of Changes	7-C	7-P	5 times 7-P, twice 7-C
AI7.7 Final Acceptance Test	7-C	7-P	5 times 7-P, twice 7-C
AI7.8 Promotion to Production	1-P	1-P	OK
AI7.9 Software Release	6-C	6-P	6 times 6-P, once 6-C
AI7.10 System Distribution	6-C	6-P	OK
AI7.11 Recording and Tracking of Changes	1-D	1-D	OK
AI7.12 Post-implementation Review	7-C	7-C	OK
DS1.1 Service Level Management Framework	7-P	7-P	OK
DS1.2 Definition of Services	4-P	7-P	6 times 7-P, once 4-P
DS1.3 Service Level Agreements	7-P	7-P	OK
DS1.4 Operating Level Agreements	7-P	7-P	OK
DS1.5 Monitoring and Reporting of Service Level Achievements	7-D	7-D	OK
DS1.6 Review of Service Level Agreements and Contracts	7-C	7-C	OK
DS2.1 Identification of All Supplier Relationships	7-P	7-P	OK
DS2.2 Supplier Relationship Management	7-P	7-P	OK
DS2.3 Supplier Risk Management	7-D	7-P	OK
DS2.4 Supplier Performance Monitoring	7-D	7-D	OK
DS3.1 Performance and Capacity Planning	7-D	7-P	OK
DS3.2 Current Capacity and Performance	7-C	7-D	OK
DS3.3 Future Capacity and Performance	7-P	7-P	OK
DS3.4 IT Resources Availability	6-P	6-P	OK
DS3.5 Monitoring and Reporting	7-D	7-D	OK
DS4.1 IT Continuity Framework	6-P	6-P	OK
DS4.2 IT Continuity Plans	6-P	6-P	OK
DS4.3 Critical IT Resources	6-P	6-P	OK
DS4.4 Maintenance of the IT Continuity Plan	6-D	6-P	5 times 6-P, twice 6-D
DS4.5 Testing of the IT Continuity Plan	6-C	6-C	OK
DS4.6 IT Continuity Plan Training	3-P	6-P	6 times 6-P, once 7-P
DS4.7 Distribution of the IT Continuity Plan	4-P	4-P	OK
DS4.8 IT Services Recovery and Resumption	7-C	7-P	OK
DS4.9 Offsite Backup Storage	5-P	5-P	OK
DS4.10 Post-resumption Review	6-P	6-C	OK

DS5.1 Management of IT Security	4-P	4-P	OK
DS5.2 IT Security Plan	4-P	4-P	OK
DS5.3 Identity Management	1-P	1-P	OK
DS5.4 User Account Management	1-P	1-P	OK
DS5.5 Security Testing, Surveillance and Monitoring	7-P	7-P	OK
DS5.6 Security Incident Definition	6-P	6-P	OK
DS5.7 Protection of Security Technology	5-P	5-P	OK
DS5.8 Cryptographic Key Management	2-P	2-P	OK
DS5.9 Malicious Software Prevention, Detection and Correction	2-D	2-D	OK
DS5.10 Network Security	2-P	2-P	OK
DS5.11 Exchange of Sensitive Data	2-P	2-P	OK
DS6.1 Definition of Services	7-D	7-D	OK
DS6.2 IT Accounting	7-D	7-D	OK
DS6.3 Cost Modelling and Charging	7-P	7-P	OK
DS6.4 Cost Model Maintenance	7-C	7-C	OK
DS7.1 Identification of Education and Training Needs	3-D	3-D	OK
DS7.2 Delivery of Training and Education	3-C	3-C	OK
DS7.3 Evaluation of Training Received	3-D	3-D	OK
DS8.1 Service Desk	6-P	6-P	OK
DS8.2 Registration of Customer Queries	6-P	6-P	OK
DS8.3 Incident Escalation	6-C	6-P	OK
DS8.4 Incident Closure	6-C	6-D	6 times 6-D, once 6-P
DS8.5 Trend Analysis	6-D	6-D	OK
DS9.1 Configuration Repository and Baseline	6-D	6-P	OK
DS9.2 Identification and Maintenance of Configuration Items	6-C	6-P	OK
DS9.3 Configuration Integrity Review	6-D	6-D	OK
DS10.1 Identification and Classification of Problems	6-D	6-P	OK
DS10.2 Problem Tracking and Resolution	6-C	6-C	OK
DS10.3 Problem Closure	6-C	6-D	OK
DS10.4 Integration of Change, Configuration and Problem Management	6-P	6-P	OK
DS11.1 Business Requirements for Data Management	4-P	4-P	OK
DS11.2 Storage and Retention Arrangements	4-P	4-P	OK
DS11.3 Media Library Management System	5-P	5-P	OK
DS11.4 Disposal	5-P	5-P	OK
DS11.5 Backup and Restoration	6-P	6-P	OK
DS11.6 Security Requirements for Data Management	4-P	4-P	OK
DS12.1 Site Selection and Layout	5-P	5-P	OK
DS12.2 Physical Security Measures	5-P	5-P	OK
DS12.3 Physical Access	5-P	5-P	OK
DS12.4 Protection Against Environmental Factors	5-P	5-P	OK
DS12.5 Physical Facilities Management	5-D	5-P	OK
DS13.1 Operations Procedures and Instructions	4-P	4-P	OK
DS13.2 Job Scheduling	7-P	7-P	OK
DS13.3 IT Infrastructure Monitoring	7-D	7-D	OK
DS13.4 Sensitive Documents and Output Devices	5-P	5-P	OK

DS13.5 Preventive Maintenance for Hardware	5-P	5-P	OK
ME1.1 Monitoring Approach	7-P	7-P	OK
ME1.2 Definition and Collection of Monitoring Data	7-P	7-P	OK
ME1.3 Monitoring Method	7-P	7-P	OK
ME1.4 Performance Assessment	7-D	7-D	OK
ME1.5 Board and Executive Reporting	7-D	7-D	OK
ME1.6 Remedial Actions	7-C	7-C	OK
ME2.1 Monitoring of Internal Control Framework	7-D	7-D	OK
ME2.2 Supervisory Review	7-D	7-D	OK
ME2.3 Control Exceptions	7-D	7-D	OK
ME2.4 Control Self-assessment	7-D	7-D	OK
ME2.5 Assurance of Internal Control	7-D	7-D	OK
ME2.6 Internal Control at Third Parties	7-D	7-D	OK
ME2.7 Remedial Actions	7-C	7-C	OK
ME3.1 Identification of Laws and Regulations Having Potential Impact on IT	7-D	7-P	OK
ME3.2 Optimization of Response to Regulatory Requirements	7-C	7-C	OK
ME3.3 Evaluation of Compliance With Regulatory Requirements	7-D	7-D	OK
ME3.4 Positive Assurance of Compliance	7-P	7-P	OK
ME3.5 Integrated Reporting	7-D	7-D	OK
ME4.1 Establishment of an IT Governance Framework	4-P	4-P	OK
ME4.2 Strategic Alignment	4-P	4-P	OK
ME4.3 Value Delivery	7-P	4-P	OK
ME4.4 Resource Management	7-P	4-P	OK
ME4.5 Risk Management	7-D	4-D	OK
ME4.6 Performance Measurement	7-D	7-D	OK
ME4.7 Independent Assurance	7-C	7-C	6 times 7-C, once 7-D

APPENDIX C

ADDITIONAL CONTROL OBJECTIVES FROM BEST PRACTICES

Table 21: Additional Control Objectives from Best Practices

Best Practice	Control Objective in Best Practice	Mapping
ISO27001	A.6.1.4 Authorization process for information processing facilities	1-P
ISO27001	A.8.3.2 Return of assets	1-P
ISO27001	A.9.2.7 Removal of property	1-P
ISO27001	A.10.1.4 Separation of development, test and operational facilities	1-P
ISO27001	A.10.6.2 Security of network services	1-P
ISO27001	A.10.7.3 Information handling procedures	1-P
ISO27001	A.10.7.4 Security of system documentation	1-P
ISO27001	A.10.10.1 Audit logging	1-D
ISO27001	A.10.10.3 Protection of log information	1-P
ISO27001	A.10.10.4 Administrator and operator logs	1-D
ISO27001	A.10.10.5 Fault logging	1-D
ISO27001	A.11.1.1 Access control policy	1-P
ISO27001	A.11.2.2 Privilege management	1-P
ISO27001	A.11.2.3 User password management	1-P
ISO27001	A.11.3.1 Password use	1-P
ISO27001	A.11.3.3 Clear desk and clear screen policy	1-P
ISO27001	A.11.4.5 Segregation in networks	1-P
ISO27001	A.11.4.6 Network connection control	1-P
ISO27001	A.11.4.7 Network routing control	1-P
ISO27001	A.11.5.1 Secure log-on procedures	1-P
ISO27001	A.11.5.3 Password management system	1-P
ISO27001	A.11.5.4 Use of system utilities	1-P
ISO27001	A.11.5.5 Session time-out	1-P
ISO27001	A.11.5.6 Limitation of connection time	1-P
ISO27001	A.11.6.1 Information access restriction	1-P
ISO27001	A.12.4.2 Protection of system test data	1-P
ISO27001	A.12.4.3 Access control to program source code	1-P
BS7799	4.6.7.2 Security of media in transit	2-P
BS7799	4.6.7.3 Electronic commerce security	2-P
BS7799	4.6.7.4 Security of electronic mail	2-P
BS7799	4.6.7.6 Publicly available systems	2-P
BS7799	4.6.7.7 Other forms of information exchange	2-P
BS7799	4.7.4.2 Enforced path	2-D
BS7799	4.7.4.3 User authentication for external connections	2-P
BS7799	4.7.4.4 Node authentication	2-P
BS7799	4.7.4.5 Remote diagnostic port protection	2-P
BS7799	4.7.8.1 Mobile computing	2-P
BS7799	4.7.8.2 Teleworking	2-P

BS7799	4.8.2.3 Message authentication	2-P
BS7799	4.8.3.2 Encryption	2-P
BS7799	4.8.3.3 Digital signatures	2-P
BS7799	4.10.1.6 Regulation of cryptographic controls	2-D
ISO27001	A.7.1.1 Inventory of assets	5-P
ISO27001	A.7.1.2 Ownership of assets	5-P
ISO27001	A.7.1.3 Acceptable use of assets	5-P
ISO27001	A.9.1.3 Securing offices, rooms and facilities	5-P
ISO27001	A.9.1.5 Working in secure areas	5-P
ISO27001	A.9.1.6 Public access, delivery and loading areas	5-P
ISO27001	A.9.2.2 Supporting utilities	5-P
ISO27001	A.9.2.3 Cabling security	5-P
ISO27001	A.9.2.5 Security of equipment offpremises	5-P
ISO27001	A.11.3.2 Unattended user equipment	5-P
ISO27001	A.15.1.3 Protection of organizational records	5-P
ISO27001	A.15.3.2 Protection of information systems audit tools	5-P
ITIL	Design and implement technical migration plans	6-P
ITIL	Roll-out ICT solutions	6-P
ITIL	Provide technical guidance and specialist support	6-P
ITIL	Assess IT capabilities	6-D
ITIL	Plan deployment	6-P
ITIL	Plan handover and support	6-P
ITIL	Maintain CMDB and CDB	6-P
ITIL	Understand resource usage and workflow	6-D
ITIL	Prepare and maintain capacity plan	6-P
ITIL	Formulate availability and recovery design criteria	6-P
ITIL	Review IT service and component availability	6-D
ITIL	Consider security requirements	6-P
ITIL	Improve availability within cost constraints	6-C
ITIL	Plan and design service desk infrastructure	6-P
ITIL	Specify targets and effectiveness metrics	6-P
ITIL	Determine service desk functions	6-P
ITIL	Resource and manage service desk effectively	6-P
ITIL	Control problems	6-D
ITIL	Assess infrastructure errors	6-D
ITIL	Control errors	6-D
ITIL	Undertake major problem reviews	6-C
ITIL	Establish CMDB and DSL	6-P
ITIL	Maintain and track CI status	6-D
ITIL	Verify and audit CIs against CMDB records	6-D
ITIL	Maintain forward schedule of change	6-D
ITIL	Review change	6-P
ITIL	Release design, build and configuration	6-P
ITIL	Roll-out planning	6-P
ITIL	Release review	6-P